ZXR10
Router/Ethernet Switch
Alarm Handling Manual

Version 4.8.23

ZTE CORPORATION
ZTE Plaza, Keji Road South,
Hi-Tech Industrial Park,
Nanshan District, Shenzhen,
P. R. China
518057
Tel: (86) 755 26771900
Fax: (86) 755 26770801
URL: http://ensupport.zte.com.cn
E-mail: support@zte.com.cn

LEGAL INFORMATION

Copyright © 2006 ZTE CORPORATION.

The contents of this document are protected by copyright laws and international treaties. Any reproduction or distribution of this document or any portion of this document, in any form by any means, without the prior written consent of ZTE CORPORATION is prohibited. Additionally, the contents of this document are protected by contractual confidentiality obligations.

All company, brand and product names are trade or service marks, or registered trade or service marks, of ZTE CORPORATION or of their respective owners.

This document is provided "as is", and all express, implied, or statutory warranties, representations or conditions are disclaimed, including without limitation any implied warranty of merchantability, fitness for a particular purpose, title or non-infringement. ZTE CORPORATION and its licensors shall not be liable for damages resulting from the use of or reliance on the information contained herein.

ZTE CORPORATION or its licensors may have current or pending intellectual property rights or applications covering the subject matter of this document. Except as expressly provided in any written license between ZTE CORPORATION and its licensee, the user of this document shall not acquire any license to the subject matter herein.

ZTE CORPORATION reserves the right to upgrade or make technical change to this product without further notice.

Users may visit ZTE technical support website http://ensupport.zte.com.cn to inquire related information.

The ultimate right to interpret this product resides in ZTE CORPORATION.

Revision History

Revision No.	Revision Date	Revision Reason
R1.0	Oct.16th, 2009	First Edition

Serial Number: sjzl20095779

Contents

About This Manual i

Alarm Overview 1

Overview 1

Alarm Glossry Overview 1

Message No. 1

Default Severity Level 2

Alarm Recovery 2

Alarm Type 2

NM Level 3

Cause 3

Related Alarms 4

Recommended Operations 4

Alarm Prototype Description 5

Alarm Description 5

Supported device type 5

Appendix Description 5

Message Format Description 5

Alarm Message 9

Hardware alarm 9

Environment Alarm 9

63 9

64 10

65 11

66 12

67 13

68 14

69 15

73 16

74 17

75 18

79 19

80 20
Board Alarms 22
279 22
293 22
299 22
300 23
301 24
302 24
303 25
310 26
311 26
312 27
313 28
Port Alarm 29
512 29
540 29
541 29
542 29
Software Alarm 30
ETHOAM Alarm 30
16128 30
16129 31
16130 31
16131 32
30464 34
30465 35
30466 36
30467 37
ROS Alarm 38
16384 38
16386 38
16389 38
16391 38
16392 39
16393 39
16394 40
16395 41
16396 41
DATABASE Alarm 42
16640 42

16642 42
16643 43
16644 43
16645 43
16646 43
OAM Alarm 44
16899 44
16900 44
16901 45
16903 46
16904 46
16905 46
16906 46
16907 46
16916 47
16917 47
16918 47
16919 48
16920 48
16921 49
16922 49
16923 49
16924 50
16925 50
16926 51
OSPF Alarm 52
17408 52
17409 52
17410 52
17411 53
17412 53
17413 53
17414 53
17415 53
17416 54
17417 54
17418 54
17419 54
17420 55
17421 55

17422 55
17423 55
17424 55
17425 56
17426 56
17427 56
17428 56
17429 56
RIP Alarm 57
17664 57
17666 57
17667 57
17670 57
17671 58
17672 58
17673 58
17676 58
17677 59
BGP Alarm 59
17920 59
17921 59
17922 59
17923 59
17924 60
17925 60
17927 60
17928 60
17932 61
17934 61
17936 61
17938 61
17940 61
17941 62
17942 62
17943 62
17944 62
17945 62
17946 63
17947 63
17949 63

17950 63
17951 63
17952 64
17953 64
17954 64
17955 64
17956 64
17957 65
17958 65
17959 65
17960 65
17961 65
17962 66
17963 66
17964 66
DRP Alarm 66
18176 66
18177 66
18180 67
18181 67
18182 67
18183 67
18184 68
18185 68
18186 68
18189 68
18190 68
18191 69
18192 69
18193 69
18195 69
18196 70
TCP Alarm 71
18433 71
18434 71
18435 71
18436 71
18437 71
18438 72
18439 72

18440 72
18450 72
18451 72
18452 73
18453 73
18455 73
18456 73
18457 73
18458 74
18459 74
18460 74
18461 74
18463 74
18464 75
UDP Alarm 75
18560 75
18561 75
18562 75
18563 75
18564 76
IP Alarm 76
18689 76
18691 76
18692 76
18720 77
18721 77
18722 77
18737 77
18738 77
18739 78
18740 78
18741 78
18742 78
18743 78
18744 79
18745 79
18752 79
18754 79
18784 79
18785 80

18786 80
18787 80
18790 80
18791 80
18794 81
18832 81
18833 82
18834 82
18835 83
IGMP Alarm 83
18944 83
18945 84
ARP Alarm 84
19712 84
19713 84
19714 84
19715 85
19716 85
19717 85
19720 85
IS-IS Alarm 86
19968 86
19969 86
19970 86
19972 87
19974 87
19975 87
19976 87
19977 87
19978 88
19979 88
19980 88
19981 88
19982 88
19983 89
RMON Alarm 90
20737 90
20746 90
20747 90
20748 90

20757 91
20758 91
20759 91
20776 91
20793 91
URPF Alarm 92
21248 92
ACL Alarm 92
21762 92
21764 92
21773 92
21774 93
21775 93
21776 93
21777 94
VRRP Alarm 95
22016 95
MAC Alarm 95
22784 95
22785 95
22786 95
22787 96
22788 96
22789 96
22790 96
22792 96
22793 97
22794 97
22795 98
22796 98
22797 99
22798 99
Loop Detect 100
23296 100
DHCP Alarm 100
23808 100
23809 100
23810 101
23811 101
23812 102

23813 103
23814 103
23815 104
23816 104
23817 105
23818 105
23819 106
23820 106
23821 107
23822 107
23823 108
23824 108
MLD Alarm 109
24064 109
24065 109
STP Alarm 109
24320 109
24321 110
24322 110
24323 110
24327 110
LOCAL ACCOUNTING Alarm..... 111
24832 111
LDP Alarm 111
25344 111
25347 112
25349 112
25351 113
25354 113
25355 113
25356 113
25357 114
L2VPN Alarms 114
25856 114
25857 114
25858 114
25859 114
25863 115
25864 115
ZESR Alarms..... 115

26368 115
26369 115
26370 116
26371 116
26372 116
26373 116
26374 116
26375 117
26376 117
TACACS Alarms 117
28160 117
28161 117
28162 118
28163 118
28164 118
28165 118
28166 118
28167 119
28168 119
28169 119
AAA Alarms 119
28418 119
28419 120
28421 120
28422 120
28423 120
28429 120
MIX Alarms 121
29952 121
29953 121
29954 121
29955 122
29956 122
29957 123
29958 123
29959 124
29960 124
BFD alarm 125
30208 125
30209 126

30210 126
30212 127
30213 127
UDLD Alarm 128
29696 128
29697 128
29698 129
29699 129
MUX Alarm 130
29440 130
ZESS Alarm 130
32512 130
32513 131
32514 131
POE Alarm 132
30720 132
30721 133
ESM Alarm 134
26385 134
EPON Alarm 134
33280 134
33281 135
33282 136
33283 137
33284 137
33285 138
33286 138
33287 139
33288 140
33289 140
33290 141
33291 142
33292 142
33293 143
33294 143
33295 144
33296 144
33297 145
Command Configuration Error Prompt Messages 147

Message Format 147
Error Message Description 147
10 147
11 147
12 147
13 148
14 148
15 148
16 148
17 148
18 149
19 149
20 149
21 149
22 149
23 150
24 150
25 150
26 150
27 150
28 151
29 151
30 151
31 151
33 151
34 151
35 152
36 152
37 152
38 152
39 152
40 153
41 153
42 153
44 153
100 154
101 154
102 154
103 154
104 154

105 154
106 155
107 155
108 155
109 155
110 155
112 155
201 156
202 156
203 156
204 156
206 156
207 157
208 157
209 157
210 157
211 157
212 158
213 158
214 158
215 158
216 158
217 159
218 159
219 159
220 159
221 159
222 160
223 160
224 160
225 160
226 160
227 160
228 161
229 161
230 161
231 161
232 161
233 162
235 162

236 162
237 162
238 162
239 162
240 163
241 163
242 163
243 163
244 163
245 164
246 164
247 164
248 164
250 164
251 164
252 165
253 165
254 165
255 165
256 165
257 166
258 166
259 166
260 166
261 166
262 166
263 167
264 167
265 167
266 167
267 167
268 168
269 168
270 168
271 168
272 168
273 168
274 169
275 169
276 169

277 169
278 169
279 170
280 170
284 170
285 170
288 170
289 171
290 171
292 171
300 171
303 171
305 172
306 172
307 172
308 172
309 172
1001 173
1002 173
1003 173
1004 173
1005 173
1006 173
1007 174
1008 174
1009 174
1010 174
1011 174
1012 175
1013 175
1014 175
1015 175
1016 175
1017 176
1018 176
1019 176
1020 176
1021 176
1022 176
1024 177

1025 177
1026 177
1027 177
1028 177
1029 177
1030 178
1031 178
1032 178
1033 178
1034 178
1035 179
1036 179
1037 179
1038 179
1039 179
1040 179
1041 180
1042 180
1043 180
1044 180
1049 180
1050 181
1051 181
1052 181
1053 181
1054 181
1055 181
1056 182
1057 182
1058 182
1059 182
1060 182
1061 183
1062 183
1063 183
1064 183
1070 183
1071 183
1072 184
1073 184

1074 184
1080 184
1081 184
1082 185
1083 185
1500 185
1501 185
1502 185
1503 185
1504 186
1505 186
1700 186
2001 186
2002 186
2003 187
2004 187
2005 187
2006 187
2007 187
2008 188
2009 188
2010 188
2011 188
2012 188
2013 188
2014 189
2015 189
2016 189
2017 189
2018 189
2019 190
2020 190
2021 190
2022 190
2023 190
2024 190
2025 191
2026 191
2027 191
2028 191

2029 191
2030 191
2031 192
2032 192
2033 192
2034 192
2035 192
2036 193
2037 193
2038 193
2039 193
2040 193
2041 194
2042 194
2043 194
2044 194
2045 194
2046 194
2047 195
2048 195
2049 195
2050 195
2051 195
2052 195
2053 196
2054 196
2055 196
2056 196
2057 196
2058 197
2059 197
2060 197
2200 197
2801 197
2802 198
2803 198
2804 198
2805 198
2806 198
2807 198

2808 199
2809 199
2810 199
2811 199
2812 199
2813 199
2814 200
2815 200
3001 200
3002 200
3003 200
3004 201
3005 201
3006 201
3007 201
3008 201
3009 201
3010 202
3011 202
3012 202
3013 202
3014 202
3015 203
3016 203
3017 203
3018 203
4001 203
4002 203
4003 204
4004 204
4005 204
4006 204
4007 204
4008 204
4009 205
4010 205
4011 205
4012 205
4013 205
4014 205

4015 206
4016 206
4030 206
4031 206
4032 206
4033 207
4034 207
4035 207
4036 207
4037 207
4038 207
4039 208
4040 208
4041 208
4042 208
4043 208
4044 209
4045 209
4046 209
4047 209
4048 209
4049 209
4501 210
4502 210
4503 210
4504 210
4505 210
4506 211
4507 211
4508 211
4509 211
4510 211
4511 212
4512 212
5001 212
5002 212
5003 212
5004 213
5005 213
5006 213

5007 213
6001 213
6010 213
6011 214
6012 214
6020 214
6021 214
6022 214
6023 215
6024 215
6025 215
6026 215
6027 215
6028 215
6029 216
6030 216
6031 216
6032 216
6033 216
6034 216
6035 217
6036 217
6037 217
6038 217
6040 217
6050 217
6051 218
6052 218
6053 218
6054 218
6055 218
6056 219
6057 219
6058 219
6059 219
6080 219
6081 220
6082 220
6083 220
6084 220

6085 220
6086 220
6087 221
6088 221
6089 221
6601 221
7001 221
7002 221
7003 222
7004 222
7005 222
7006 222
7007 222
7008 222
7010 223
7011 223
7012 223
7020 223
7021 223
7022 223
7023 224
7024 224
7030 224
7031 224
7032 224
7040 224
7041 225
7042 225
7050 225
7051 225
7052 225
7053 225
7061 226
7062 226
7063 226
7064 226
7065 226
7066 226
7067 227
7068 227

7069 227
7071 227
7081 227
7082 227
7083 228
7091 228
8008 228
8009 228
8010 228
8011 228
8501 229
8502 229
8503 229
8504 229
8505 229
8506 229
8509 230
8510 230
8511 230
8512 230
8513 230
8514 231
8515 231
8516 231
8517 231
8601 231
8602 231
8603 232
8604 232
8605 232
8606 232
8607 232
8608 233
8609 233
8610 233
8611 233
8612 233
8613 233
8614 234
8615 234

8616 234
8617 234
8618 234
8619 234
8620 235
8621 235
8622 235
8623 235
8624 235
8625 236
8626 236
8701 236
8702 236
8703 236
8704 236
8705 237
8706 237
8707 237
8708 237
8801 237
8802 238
8803 238
8804 238
8805 238
8806 238
8901 238
8903 239
8904 239
8905 239
8906 239
8907 239
8908 239
8909 240
8910 240
8911 240
8912 240
8913 240
8914 240
8915 241
8916 241

8917 241
8918 241
8919 241
8951 242
8952 242
8953 242
8954 242
8955 242
8956 243
9001 243
9002 243
9003 243
9004 243
9005 243
9101 244
9102 244
9103 244
9105 244
9106 244
9201 244
9202 245
9203 245
9204 245
9501 245
9502 245
9503 246
9506 246
9507 246
9508 246
9510 246
9511 247
9512 247
9513 247
9514 247
9515 247
9516 247
9517 248
9518 248
9519 248
9520 248

9521 248
9522 249
9523 249
9601 249
9602 249
9603 249
9604 250
9605 250
9606 250
9607 250
12401 250
12402 250
12403 251
12404 251
12405 251
12406 251
12407 251
12409 252
12410 252
12411 252
12420 252
12421 252
12422 252
12423 253
12424 253
12425 253
12426 253
12427 253
12428 253
12429 254
12430 254
12431 254
12432 254
12433 254
30201 254
30202 255
30203 255
30204 255
30205 255
30206 255

30207 256
30208 256
TRAP Messages 257
TRAP Message Explanation 257
System TRAP Message 257
coldStart 257
warmStart 258
authenticationFailure 258
linkUp 258
linkDown 259
Alarm TRAP Message 259
Hardware Alarm Trap 259
Software Alarm Trap 260
RMON TRAP Message 261
risingAlarm Trap 261
fallingAlarm Trap 261
OSPF TRAP Message 262
ospfVirtIfStateChange 262
ospfNbrStateChange 262
ospfVirtNbrStateChange 263
ospfIfConfigError 264
ospfVirtIfConfigError 264
ospfIfAuthFailure 265
ospfVirtIfAuthFailure 266
ospfIfRxBadPacket 266
ospfVirtIfRxBadPacket 267
ospfTxRetransmit 267
ospfVirtIfTxRetransmit 268
ospfOriginateLsa 269
ospfMaxAgeLsa 269
ospfLsdbOverflow 270
ospfLsdbApproachingOverflow 270
ospfIfStateChange 271
BGP TRAP Message 271
bgpEstablished 271
bgpBackwardTransition 271
DHCP TRAP Message 272
online 272
offline 272
VRRP TRAP Message 273

vrrpTrapAuthFailure 273
vrrpTrapNewMaster 273
IPv6TRAP Information 274
ipv6IfStateChange 274
POE TRAP Information 274
pethPsePortOnOffNotification 274
pethMainPowerUsageOnNotification 275
pethMainPowerUsageOffNotification 275

About This Manual

Purpose

The manual is ZXR10 Router/Ethernet Switch Message Manual and suited for following equipments.

- ZXR10 GAR universal access router (shorted as ZXR10 GAR)
- ZXR10 GER universal high-performance router (shorted as ZXR10 GER)
- ZXR10 T64E/T128 carrier class high-end router (shorted as ZXR10 T64E/T128)
- ZXR10 3900/3200 series intelligent Ethernet switches (shorted as ZXR10 3900/3200)
- ZXR10 5900/5200 series all gigabit-port intelligent routing switch (shorted as ZXR10 5900/5200)
- ZXR10 T160G/T64G/T40G 10G MPLS routing switch (shorted as ZXR10 T160G/T64G/T40G)
- ZXR10 8900 series 10G MPLS routing switch (shorted as ZXR10 8900)

The manual content is based on unified ZXROS platform and suited to all equipments if with no special note or described as ZXR10. In the manual, the contents describing router are also applied to the switches with route function.

Intended Audience

This manual is intended for engineers and technicians who perform operation activities on ZXR10 Router/Ethernet Switch.

What Is in This Manual

This manual describes alarm messages that may appear during the operation of ZXR10 router/Ethernet switch, command configuration error prompt messages that may appear during configuration, as well as TRAP messages sent by the router.

This manual contains the following chapters:

Chapter	Summary
Chapter 1, Alarm Overview	This chapter describes the alarm message format on ZXR10 Router/Ethernet Switch.
Chapter 2, Alarm Message	This chapter describes the alarm messages appeared on ZXR10 data product, including hardware alarm and software alarm.
Chapter 3, Command Configuration Error Prompt Messages	This chapter describes the error prompt message appeared during command configuration.
Chapter 4, TRAP Message	This chapter describes all TRAP messages sent by system.

This page is intentionally blank.

Chapter 1

Alarm Overview

Table of Contents

Overview 1
Alarm Glossry Overview 1
Message Format Description 5

Overview

The alarm management is responsible for gathering the malfunction and the event information which appears in the system running and the handling of traffic process. Real-time display or storage into the database is executed in form of alarm or notice on the user-oriented alarm monitoring platform. It also provided the interface direct-viewing monitoring or the historical inquiry method to reflect the current or the past system running status and the handling of traffic process. All of these helped the maintenance personnel to do the troubleshooting and take preventive measures, so that the system and the service restores normal as soon as possible.

Alarm Glossry Overview

Message No.

Message No. is also named alarm code. It is the unique identification to distinguish alarms. It includes foreground alarm and backgroud alarm. The foreground alarm code is a fixed value defined by macro for distinguishing alarms. Because alarm and the corresponding recovery use the same alarm code, only alarm code and notice code need to be defined. The alarm source provides the macro name in the alarm code identifier macro column. The background alarm code is used to display in alarm monitoring platform and is mapping with the foreground alarm code one by one according to some rules.

Default Severity Level

ZXR10 devices alarm level includes the following 8 levels:

- Severity 1: emergency messages EMERGENCIES, the system is unusable.
- Severity 2: alert messages ALERTS. Magnitude malfunction appears in the system and immediate action is needed.
- Severity 3: critical messages CRITICAL. Emergency condition appears.
- Severity 4: error messages ERRORS. Error condition appears.
- Severity 5: warning messages WARNINGS. The system prompts that warnings appear.
- Severity 6: notification messages NOTIFICATIONS. The normal but significant event information that the system notifies to each part and records.
- Severity 7: informational messages INFORMATIONAL. It is only an informational message.
- Severity 8: debugging messages DEBUGGING. It is the respondse information type when the administrator debugs the system or network .

  Alarm level includes the default and actual level. The default level is the original alarm level and it is fixed. Users can not modify it. The actual alarm level is the one used in the process of device running which is equal to the default level. Users can modify it using the command **alarm level-change** <*alarm-code*><*level*>. Only alarm levels 4–8 can be modified.

Alarm Recovery

Alarm recovery includes "available" and "unavailable". "available" means that a prompt will appear when this alarm is deleted. "unavailable" means that there is no prompt when this alarm is deleted.

Alarm Type

Alarm type includes the following six categories.

- "CommunicationAlarm"
- "ProcessingErrorAlarm"
- "QOSAlarm"
- "EquipmentAlarm"
- "EnvironmentalAlarm"
- "OMSAlarm"

NM Level

NM level includes level 1, level 2, level 3, level 4 and level 5. The meanings for each level are as follows.

- Level 1: critical
- Level 2: major
- Level 3: minor
- Level 4: clear
- Level 5: informational

Cause

Various kinds of causes are as follows. In order to recover the system as soon as possible, we should find out trigger conditions, trigger frequency, the resolutions and the prevent measures. The causes for ZXR10 alarm messages are as follows:

1. The hardware or device malfunction.
   i. Single board malfunction.
   ii. Other hardware malfunction, such as system power malfuncrion, fan malfunction, flash card malfunction and so on.
   iii. Hardware can not satisfy needs. For example, current hardware such as single board, CPU and the memory can not satisfy the increasing needs.
2. Software malfunction. It may be the software BUG or the failure caused by the software upgrade.
3. Environment alarm. For example,
   i. The smooth running of the system has a strict requirment on the environment. If the temprature or the humidity can not satisfy the requirment, alarm occurs.
   ii. Natural disaster and the accidental incident can also generate alarms. For example, lightening, fire or earthquake.
4. The configuration error or the improper setup.
   i. The setup problem: the interface setup between devices, the system privilege, password, file and catolog setup.
   ii. The configuration can not satisfy the system requirments: the system capability and capacity decrease caused by configuration error. Especially if the alarm threshold is set by users, proper configuration is strongly required.
5. The malfunction on the other end device also generates alarms.

Related Alarms

If there is some alarms that are related to this one, such as the source alarm that generates this one and the alarms caused by this one, please list them.

Recommended Operations

This section lists the recommended operations that can remove the alarms .

1. The general analysis methods for the alarms are as follows.
   i. Read the alarm message, information description carefully and refer to the related content in this manual.
   ii. Check whether the network connection is normal using network commands such as ping, telnet, netstat, ipconfig/ifconfig, route, trace/tracert and so on.
   iii. View the related data configuration directly to check whether there is error, missed or unreasonable configurations.
   iv. For more difficult problems, analyse them with the network protocol analysis software "sniffer".
   v. For possible hardware malfunction, replace this hardware with the same available hardware to help the manager to determine whether the malfunction is from the software or the hardware.
2. The general disposal methods for the alarms are as follows.
   i. For hardware or device malfunction, contact with ZTE service staff to replace it. For malfunctions such as "hardware dissatisfactory", add the hardware or replace the low capacity parts.
   ii. For software or the system malfunctions, upgrade or downgrade the software version. Backup the configuration before version upgrading.
   iii. For alarms caused by the environment, please check and resolve the problems in time according to alarm failure and alarm message. Avoide or reduce the direct or physical damage for the device caused by the environment.
   iv. For system setup and configuration problems, check where the malfunction is and modify the configuration . For alarms caused by error input commands, please view the online command "help" or refer to related manual and execute it after inputting this command again.
   v. For alarms caused by the other end, inform the other end of the displayed alarm message and assist in resolving this problem. And then check and inform the other end whether this alarm is removed.
3. For alarms that can not be resolved by users, contact with ZXR10 router professors of ZTE corporation or call our cus-

tomer support center at 800-830-1118(for free) , 400-830-1118(modename for free) and 0711-65000(military network).

4. The subsequent steps to dispose the alarms are as follows.
   i. Check whether the alarm is removed. The methods include: the alarm message does not appear or the normal system alarm appears; reboot the single board or this module; the service recovers to normal.
   ii. Remember to record the detailed "alarm processing log" which includes alarm phenomenon, alarm cause and the disposal methods. The "alarm processing log" is convenient for resolving the similar problems.

Alarm Prototype Description

It is the alarm instance that is the display information on the rack when the alarm occurs. This is shown by the command **show logging alarm**.

Alarm Description

Alarm description is the explanation for the rack alarms. It describes the malfunction on the device.

Supported device type

Supported device type lists all the device types that supports this alarm.

Appendix Description

Appendix Description list all the points that should pay attention to. for example, explain that there is difference of this alarm between versions and devices.

Message Format Description

The alarm message format is as follows.

<time> **alarm** *<number>*{**occurred** | **cleared**}*<type><description>* **sent by** *<sender>*

The following table describes each field of an alarm message.

Field	Description
<time>	Alarm generation time
number	Alarm code
occurred | **cleared**	Alarm status: "occurred" indicates that an alarm has occurred; while "cleared" indicates that the alarm has been cleared (it is only applied to hardware alarms).
type	Alarm type, which is identified with %.
<description>	Alarm message description
sender	Alarm message sender

Note:

Alarm messages in the "cleared" status are merely system recovery messages, which need no operation.

ZXR10 alarm messages have 2 types, hardware alarm and software alarm. Of which, the 2 types may be divided further into more sub-types.

- Hardware alarms can be divided into environment alarms, board alarms and port alarms.
- Software alarms may be separated as more sub-types as ROS, DATABASE, OSPF, RIP, BGP, DRP, TCP, UDP, IP, TELNET, ARP, ISIS, RMON, ACL, URPF, VRRP, PPP, VIRUS-SCAM and MAC.

Alarm message examples are as follows.

1. Hardware alarm
   - Environment alarm (alarm occurred)

     15: 41: 22 09/11/2003 UTC alarm 6 occurred. %ENVIRONMENT% Rack fan 1 wrong sent by UPC(MPU) 1
   - Environment alarm (alarm cleared)

     15: 51: 22 09/11/2003 UTC alarm 6 cleared. %ENVIRONMENT% Rack fan 1 normal sent by UPC(MPU) 1
   - Line board alarm (alarm occurred)

     10: 13: 36 09/15/2003 UTC alarm 279 occurred. %Board% Remove Interface from slot 3 sent by SMP 1
   - Line board alarm (alarm cleared)

     10: 13: 51 09/15/2003 UTC alarm 279 cleared. %Board% Add Interface at slot 3 sent by SMP 1
   - Port alarm (alarm occurred)

10: 12: 57 09/15/2003 UTC alarm 512 occurred. %PORT% Port Down on fei_5/6 sent by SMP 1

- Port alarm (alarm cleared)

  10: 12: 59 09/15/2003 UTC alarm 512 cleared. %PORT% Port Up on fei_5/6 sent by SMP 1

2. Software alarm

   - BGP alarm

     10: 12: 58 09/15/2003 UTC alarm 17959 occurred. %BGP% 2d18h: BGP: 100.1.1.1 went from Idle to Connect sent by SMP 1

This page is intentionally blank.

Chapter 2

Alarm Message

Table of Contents

Hardware alarm 9
Software Alarm 30

Hardware alarm

Environment Alarm

63

Message No.	63
Default Severity Level	5
Alarm Recovery	Available
Alarm Type	Environmental Alarm
NM Level	4
Cause	Board temperature is lower than the set lower threshold. The command used to set threshold for equipment temperature is: temper-threshold UPC master local lowthreshold -20 first-high-threshold 55 second-highthreshold 90
Related Alarms	64, 65
Recommended Operations	Increase environmental temperature of equipment if necessary.
Alarm Prototype Description	Alarm Occurred %s Panel %d Current local temperature is %d℃/%dF,under the low threshold(%d℃/%dF) Alarm Cleared %s Panel %d Current local temperature is %d℃/%dF,exceeds the low threshold(%d℃/%dF) The first %s is the board type, the first %d is the panel number of the board; the second %d is the centigrade temperature of the

board; the third %d is the Fahrenheit temperature of board; the fourth %d is the centigrade temperature of the set threshold and the fifth %d is the Fahrenheit temperature of the set threshold.

Alarm Occurred

%s Current local temperature is %d℃/%dF,under the low threshold(%d℃/%dF)

Alarm Cleared

%s Current local temperature is %d℃/%dF, exceeds the low threshold(%d℃/%dF)

The first %s is the board type and is fixed to BIC board. There is no panel number on BIC board, so the display format is different from other board: the first %d is the centigrade temperature of the board, the second %d is the Fahrenheit temperature of board, the third %d is the centigrade temperature of the set threshold and the fourth %d is the Fahrenheit temperature of the set threshold.

An alarm 63 level 5 occurred at 01:58:00 01/28/2001 UTC sent by UPC(MPU) 2 %ENVIRONMENT% SFC Panel 1 Current local temperature is 33℃/91F,under the low threshold(40℃/104F)

An alarm 63 level 5 cleared at 01:58:20 01/28/2001 UTC sent by UPC(MPU) 2 %ENVIRONMENT% SFC Panel 1 Current local temperature is 33℃/91F,exceeds the low threshold(-10℃/13F)

Alarm Description Board temperature is lower than the set lower threshold

Supported Devices T128/T64,T600/T1200

Appendix Specification N.A.

64

Message No. 64

Default Severity Level 5

Alarm Recovery Available

Alarm Type Environmental Alarm

NM Level 4

Cause Board temperature is higher than the set first-high temperature threshold.

The command used to set threshold for equipment temperature is:

temper-threshold UPC master local lowthreshold -20 first-highthreshold 55 second-highthreshold 90

Related Alarms 63, 65

Recommended Operations Decrease board temperature if necessary. Decrease the environment temperature of the equipment by the fan heat dissipation.

Alarm Prototype Description Alarm Occurred

%s Panel %d Current local temperature is %d℃/%dF,exceeds the first high threshold(%d℃/%dF)

Alarm Cleared

%s Panel %d Current local temperature is %d℃/%dF,under the first high threshold(%d℃/%dF)

The first %s is the board type, the first %d is the panel number of the board, the second %d is the centigrade temperature of the board, the third %d is the Fahrenheit temperature of board, the fourth %d is the centigrade temperature of the set threshold and the fifth %d is the Fahrenheit temperature of the set threshold.

Alarm Occurred

%s Current local temperature is %d℃/%dF,exceeds the first high threshold(%d℃/%dF)

Alarm Cleared

%s Current local temperature is %d℃/%dF,under the first high threshold(%d℃/%dF)

The first %s is the board type and is fixed to BIC board. There is no panel number on BIC board, so the display format is different from other board: the first %d is the centigrade temperature of the board, the second %d is the Fahrenheit temperature of board, the third %d is the centigrade temperature of the set threshold and the fourth %d is the Fahrenheit temperature of the set threshold.

An alarm 64 level 5 occurred at 01:58:30 01/28/2001 UTC sent by UPC(MPU) 2 %ENVIRONMENT% SFC Panel 1 Current local temperature is 33℃/91F,exceeds the first high threshold(30℃/86F)

An alarm 64 level 5 cleared at 01:59:20 01/28/2001 UTC sent by UPC(MPU) 2 %ENVIRONMENT% SFC Panel 1 Current local temperature is 33℃/91F,under the first high threshold(55℃/131F)

Alarm Description Board temperature is higher than the set first-high temperature threshold.

Supported Devices T128/T64,T600/T1200

Appendix Specification N.A.

65

Message No. 65

Default Severity Level 5

Alarm Recovery Available

Alarm Type Environmental Alarm

NM Level 3

Cause Board temperature is higher than the set second-high temperature threshold.

The command used to set threshold for equipment temperature is:

temper-threshold UPC master local lowthreshold -20 first-high-threshold 55 second-highthreshold 90

Related Alarms 63, 64

Recommended Operations Decrease board temperature if necessary. Decrease the environment temperature of the equipment by the fan heat dissipation. Stop using the board if the temperature is too high.

Alarm Prototype Description	Alarm Occurred %s Panel %d Current local temperature is %d℃/%dF,exceeds the second high threshold(%d℃/%dF) Alarm Cleared %s Panel %d Current local temperature is %d℃/%dF,under the second high threshold(%d℃/%dF) The first %s is the board type, the first %d is the panel number of the board, the second %d is the centigrade temperature of the board, the third %d is the Fahrenheit temperature of board, the fourth %d is the centigrade temperature of the set threshold and the fifth %d is the Fahrenheit temperature of the set threshold. Alarm Occurred %s Current local temperature is %d℃/%dF,exceeds the second high threshold(%d℃/%dF) Alarm Cleared %s Current local temperature is %d℃/%dF,under the second high threshold(%d℃/%dF) The first %s is the board type and is fixed to BIC board. There is no panel number on BIC board, so the display format is different from other board: the first %d is the centigrade temperature of the board, the second %d is the Fahrenheit temperature of board, the third %d is the centigrade temperature of the set threshold and the fourth %d is the Fahrenheit temperature of the set threshold. An alarm 65 level 5 occurred at 01:58:40 01/28/2001 UTC sent by UPC(MPU) 2 %ENVIRONMENT% SFC Panel 1 Current local temperature is 33℃/91F,exceeds the second high threshold(32℃/89F) An alarm 65 level 5 cleared at 01:58:50 01/28/2001 UTC sent by UPC(MPU) 2 %ENVIRONMENT% SFC Panel 1 Current local temperature is 33℃/91F,under the second high threshold(30℃/86F)
Alarm Description	Board temperature is higher than the set second-high temperature threshold.
Supported Devices	T128/T64,T600/T1200
Appendix Specification	N.A.

66

Message No.	66
Default Severity Level	5
Alarm Recovery	Available
Alarm Type	Environmental Alarm
NM Level	4
Cause	The CPU utilization exceeds the set memory utilization threshold. The command used to set threshold for memory utilization is (under environmental configuration mode): memory-threshold.
Recommended Operations	Use the command show process to view the CPU utilization and analyzse whether it is normal or not.

Alarm Prototype Description	Alarm Occurred %s(M) panel %d exceeds memory rate is: %3.3f%% under the alarm threshold is %d%% %s(S) panel %d exceeds memory rate is: %3.3f%% under the alarm threshold is %d%% Alarm Cleared %s(M) panel %d current memory rate is: %3.3f%% under the alarm threshold is %d%% %s(S) panel %d current memory rate is: %3.3f%% under the alarm threshold is %d%% The first %s is CPU type, the first %d is CPU SlotNo, the first %f is the current CPU utilization and the second %d is the set memory utilization threshold. An alarm 66 level 5 occurred at 01:47:50 01/28/2001 UTC sent by UPC(MPU) 2 %ENVIRONMENT% SP(M) panel 1 current memory rate is: 40.562% exceeds the alarm threshold is 2% An alarm 66 level 5 cleared at 01:48:20 01/28/2001 UTC sent by UPC(MPU) 2 %ENVIRONMENT% RP(M) panel 2 current memory rate is: 40.084% under the alarm threshold is 60%
Alarm Description	CPU utilization exceeds the set memory utilization threshold. It is 60% by default.
Supported Devices	T128/T64,T600/T1200
Appendix Specification	N.A.

67

Message No.	67
Default Severity Level	5
Alarm Recovery	Available
Alarm Type	Environmental Alarm
NM Level	4
Cause	The remote temperature is lower than the set remote lower threshold of the board. The command used to set threshold for equipment temperature: temper-threshold UPC master local lowthreshold -20 first-high-threshold 55 second-highthreshold 90.
Related Alarms	68, 69
Recommended Operations	Increase the environment temperature of the equipment if necessary.
Alarm Prototype Description	Alarm Occurred %s Panel %d Current remote temperature is %d℃/%dF,under the low threshold(%d℃/%dF) Alarm Cleared %s Panel %d Current remote temperature is %d℃/%dF,exceeds the low threshold(%d℃/%dF)

The first %s is the board type, the first %d is the panel number of the board, the second %d is the centigrade temperature of the board, the third %d is the Fahrenheit temperature of board, the fourth %d is the centigrade temperature of the set threshold and the fifth %d is the Fahrenheit temperature of the set threshold.

Alarm Occurred

%s Current remote temperature is %d℃/%dF,under the low threshold(%d℃/%dF)

Alarm Cleared

%s Current remote temperature is %d℃/%dF,exceeds the low threshold(%d℃/%dF)

The first %s is the board type and is fixed to BIC board. There is no panel number on BIC board, so the display format is different from other board: the first %d is the centigrade temperature of the board, the second %d is the Fahrenheit temperature of board, the third %d is the centigrade temperature of the set threshold and the fourth %d is the Fahrenheit temperature of the set threshold.

An alarm 67 level 5 occurred at 02:01:20 01/28/2001 UTC sent by UPC(MPU) 2 %ENVIRONMENT% SFC Panel 1 Current remote temperature is 51℃/123F, under the low threshold(56℃/132F)

An alarm 67 level 5 cleared at 02:01:30 01/28/2001 UTC sent by UPC(MPU) 2 %ENVIRONMENT% SFC Panel 1 Current remote temperature is 51℃/123F, exceeds the low threshold(-20℃/-4F)

Alarm Description The remote temperature is lower than the set remote lower threshold of the board.

Supported Devices T128/T64, T600/T1200

Appendix Specification N.A.

68

Message No. 68

Default Severity Level 5

Alarm Recovery Available

Alarm Type Environmental Alarm

NM Level 4

Cause The remote temperature is higher than the set remote first-high threshold of the board.

The command used to set threshold for equipment temperature: temper-threshold UPC master local lowthreshold -20 first-high-threshold 55 second-highthreshold 90.

Related Alarms 67, 69

Recommended Operations Decrease the board temperature if necessary. Decrease the environment temperature of the equipment by the fan heat dissipation.

Alarm Prototype Description Alarm Occurred

%s Panel %d Current remote temperature is %d℃/%dF,exceeds the first high threshold(%d℃/%dF)

Alarm Cleared

%s Panel %d Current remote temperature is %d℃/%dF,under the first high threshold(%d℃/%dF)

The first %s is the board type, the first %d is the panel number of the board, the second %d is the centigrade temperature of the board, the third %d is the Fahrenheit temperature of board, the fourth %d is the centigrade temperature of the set threshold and the fifth %d is the Fahrenheit temperature of the set threshold.

Alarm Occurred

%s Current remote temperature is %d℃/%dF,exceeds the first high threshold(%d℃/%dF)

Alarm Cleared

%s Current remote temperature is %d℃/%dF,under the first high threshold(%d℃/%dF)

The first %s is the board type and is fixed to BIC board. There is no panel number on BIC board, so the display format is different from other board: the first %d is the centigrade temperature of the board, the second %d is the Fahrenheit temperature of board, the third %d is the centigrade temperature of the set threshold and the fourth %d is the Fahrenheit temperature of the set threshold.

An alarm 68 level 5 occurred at 02:01:50 01/28/2001 UTC sent by UPC(MPU) 2 %ENVIRONMENT% SFC Panel 1 Current remote temperature is 51℃/123F,exceeds the first high threshold(40℃/104F)

An alarm 68 level 5 cleared at 02:02:10 01/28/2001 UTC sent by UPC(MPU) 2 %ENVIRONMENT% SFC Panel 1 Current remote temperature is 51℃/123F,under the first high threshold(53℃/127F)

Alarm Description The remote temperature is higher than the set remote first-high threshold of the board.

Supported Devices T128/T64,T600/T1200

Appendix Specification N.A.

69

Message No. 69

Default Severity Level 5

Alarm Recovery Available

Alarm Type Environmental Alarm

NM Level 3

Cause The remote temperature is higher than the set remote second-high threshold of the board.

The command used to set threshold for equipment temperature: temper-threshold UPC master local lowthreshold -20 first-high-threshold 55 second-highthreshold 90.

Related Alarms 67, 68

Recommended Operations	Decrease the board temperature if necessary. Decrease the environment temperature of the equipment by the fan heat dissipation. If the temperature is too high, stop using the board.
Alarm Prototype Description	Alarm Occurred %s Panel %d Current remote temperature is %d℃/%dF,exceeds the second high threshold(%d℃/%dF) Alarm Cleared %s Panel %d Current remote temperature is %d℃/%dF,under the second high threshold(%d℃/%dF) The first %s is the board type, the first %d is the panel number of the board, the second %d is the centigrade temperature of the board, the third %d is the Fahrenheit temperature of board, the fourth %d is the centigrade temperature of the set threshold and the fifth %d is the Fahrenheit temperature of the set threshold. Alarm Occurred %s Current remote temperature is %d℃/%dF,exceeds the second high threshold(%d℃/%dF) Alarm Cleared %s Current remote temperature is %d℃/%dF,under the second high threshold(%d℃/%dF) The first %s is the board type and is fixed to BIC board. There is no panel number on BIC board, so the display format is different from other board: the first %d is the centigrade temperature of the board, the second %d is the Fahrenheit temperature of board, the third %d is the centigrade temperature of the set threshold and the fourth %d is the Fahrenheit temperature of the set threshold. An alarm 69 level 5 occurred at 02:02:40 01/28/2001 UTC sent by UPC(MPU) 2 %ENVIRONMENT% SFC Panel 1 Current remote temperature is 51℃/123F,exceeds the second high threshold(50℃/122F) An alarm 69 level 5 cleared at 02:02:50 01/28/2001 UTC sent by UPC(MPU) 2 %ENVIRONMENT% SFC Panel 1 Current remote temperature is 51℃/123F,under the second high threshold(100℃/212F)
Alarm Description	The remote temperature is higher than the set remote second-high threshold of the board.
Supported Devices	T128/T64, T600/T1200
Appendix Specification	N.A.

73

Message No.	73
Default Severity Level	5
Alarm Recovery	Available
Alarm Type	Environmental Alarm
NM Level	4

Cause	The rack temperature is higher than the set single high threshold.
Influence	This leads to the abnormal working of the switch.
Recommended Operations	Lower the environment temperature of the rack by using fan heat dissipation.
Alarm Prototype Description	Alarm occured Current temperature is %dC/%dF,exceeds the threshold(%dC/%dF) Alarm cleared Current temperature is %dC/%dF,under the threshold(%dC/%dF) The first %d is the environment Centigrade degree; the second %d is the Fahrenheit degree; the third %d is the environment Centigrade degree of the set threshold; the fourth %d is the environment Fahrenheit degree of the set threshold. Alarm occured 16:20:31 06/26/2008 UTC alarm 73 occurred %ENVIRONMENT% Current temperature is 90C/194F,exceeds the threshold(80C/176F) Alarm cleared 16:22:11 06/26/2008 UTC alarm 73 cleared %ENVIRONMENT% Current temperature is 80C/176F,under the threshold(90C/194F)
Alarm Description	The rack temperature is higher than the set single high threshold.
Supported Devices	ZXR10 3900/3200, 5900/5200 and G-series switch.
Appendix Specification	N.A.

74

Message No.	74
Default Severity Level	5
Alarm Recovery	Available
Alarm Type	Environmental Alarm
NM Level	3
Cause	The power works abnormally.
Influence	This leads to the abnormal working of the switch.
Recommended Operations	Check whether the power input is normal and whether the rack output is normal; whether the power module is plugged correctly; whether the connection is OK.
Alarm Prototype Description	Alarm occured Power%d do not work! Alarm cleared Power%d restart! % d: the power serial number. Multiple power states can be displayed simultaneously. UAS10800E:

	Current Power Module %d is removed %d: power module number Alarm cleared Current Power work normal % d: the power serial number. Multiple power states can be displayed simultaneously. Example: Alarm occured 15:20:31 06/26/2008 UTC alarm 74 occurred %ENVIRONMENT% Power1 do not work! Alarm cleared 15:21:3 06/26/2008 UTC alarm 74 occurred %ENVIRONMENT% Power1 restart!
Alarm Description	The power works abnormally.
Supported Devices	ZXR10 3900/3200, 5900/5200, G-series switch and ZX-UAS-UAS10600, UAS10800E.
Appendix Specification	N.A.

75

Message No.	75
Default Severity Level	5
Alarm Recovery	Available
Alarm Type	Environmental Alarm
NM Level	4
Cause	The fan works abnormally.
Influence	This leads to the abnormal working of the switch.
Recommended Operations	Check whether the power input and output of the fan is normal; whether the fans are plugged correctly; whether the fuse is OK.
Alarm Prototype Description	Alarm occured Fan%d do not work! Alarm cleared: Fan%d restart! % d: the power serial number. Multiple power states can be displayed simultaneously. UAS10800E: Current Trunk %s Fan fail to work %s: Top or Bottom Alarm cleared Current Cabinet/Trunk Fan work normal %s: Top or Bottom

Example:

Alarm occured

15:10:11 06/26/2008 UTC alarm 75 occurred %ENVIRONMENT% Fan1 do not work!

Alarm cleared

15:13:13 06/26/2008 UTC alarm 75 occurred %ENVIRONMENT% Fan1 restart!

Alarm Description The fan works abnormally.

Supported Devices ZXR10 3900/3200, 5900/5200, G-series switch and ZX-UAS-UAS10600, UAS10800E.

Appendix Specification N.A.

79

Message No. 79

Default Severity Level 6

Alarm Recovery Available

Alarm Type Equipment Alarm

NM Level 1

Cause Power malfunction.

Influence This leads to the abnormal working of the board.

Related Alarms 76, 77

Recommended Operations Wait for our customer service personnel to deal with the power model malfunction.

Alarm Prototype Description Alarm occurred

Power errorreason%s

Alarm cleared:

Power recover: %s

%s: the cause for this malfunction

The content of %s is:

- New rack alarm(only be applied for new rack)
  i. Current Power Module 1 fail to work

     15:02:38 08/14/2008 UTC alarm 79 occurred Power error, reason: Current Power Module 1 fail to work sent by UPC(MPU)

  ii. Current Power Module 2 fail to work

     15:04:08 08/14/2008 UTC alarm 79 occurred Power error, reason: Current Power Module 2 fail to work sent by UPC(MPU) 1

  iii. Current Power Module 3 fail to work

15:06:08 08/14/2008 UTC alarm 79 occurred Power error, reason: Current Power Module 3 fail to work sent by UPC(MPU) 1

- Old rack alarm:
  i. Current Power Commutate Module 1 fail to work

     15:07:38 08/14/2008 UTC alarm 79 occurred Power error, reason: Current Power Commutate Module 1 fail to work sent by UPC(MPU) 1

  ii. Current Power Commutate Module 2 fail to work

     15:46:02 08/14/2008 UTC alarm 79 occurred Power error, reason: Current Power Commutate Module 2 fail to work sent by UPC(MPU) 1 15:46:02 08/14/2008 UTC alarm 79 occurred Power error, reason: Current Power Commutate Module 2 fail to work sent by UPC(MPU) 1

  iii. Current Power Commutate Module 3 fail to work

     15:47:32 08/14/2008 UTC alarm 79 occurred Power error, reason: Current Power Commutate Module 3 fail to work sent by UPC(MPU)1

- General alarm:
  i. The power data line isn't plugged into the bic board

     14:32:38 08/14/2008 UTC alarm 79 occurred Power error, reason: The power data line isn't plugged into the bic board sent by UPC(MPU) 1

  ii. Current Power work normal

     15:05:08 08/14/2008 UTC alarm 79 cleared Power recover: Current Power work normal sent by UPC(MPU) 1

Alarm Description Power malfunction.

Supported Devices ZXR10 T64E, T128, T600, T1200

Appendix Specification ZXR10 T64, T128 adopts old rack; ZXR10 T600, T1200 adopts new rack.

80

Message No. 80

Default Severity Level 6

Alarm Recovery Available

Alarm Type Equipment Alarm

NM Level 2

Cause Fan malfunction.

Influence This may cause heat dissipation malfunction on the rack and the temperature increment on each single board.

Recommended Operations Wait for our customer service personnel to deal with the fan malfunction.

Alarm Prototype Description

Alarm Occurred

Fan errorreason %s

Alarm Recovered:

Fan recover: %s

%s cause

- The 3 types of new rack alarms are as follows(only for new rack).
  i. The fan data line isn't plugged into the BIC board. If none of the 3 power modules are working, it implies that the power and the fan are not plugged well.

     14:51:08 08/14/2008 UTC alarm 80 occurred Fan error, reason: The fan data line isn't plugged into the bic board sent by UPC(MPU) 1

  ii. Current Trunk Top Fan fail to work

     14:44:38 08/14/2008 UTC alarm 80 occurred Fan error, reason: Current Trunk Top Fan fail to work sent by UPC(MPU) 1

  iii. Current Trunk Bottom Fan fail to work

     15:51:32 08/14/2008 UTC alarm 80 occurred Fan error, reason: Current Trunk Bottom Fan fail to work sent by UPC(MPU) 1

- The 4 types of old rack alarms are as follows(only for old rack).
  i. The fan data line isn't plugged into the BIC board. If all the fans are not working, it implies that the line of the fan is not plugged well.

     14:51:08 08/14/2008 UTC alarm 80 occurred Fan error, reason: The fan data line isn't plugged into the bic board sent by UPC(MPU) 1

  ii. Current Trunk Top Fan Num …..fail to work

     One or two of the 8 fans work abnormally. The abnormal fan number is behind Num. For example, Num 3 5.

     14:53:08 08/14/2008 UTC alarm 80 occurred Fan error, reason: Current Trunk Top Fan Num 3 4 7 8 fail to work sent by UPC(MPU) 1

  iii. Current Trunk Bottom Fan Num….. fail to work

     One or two of the 8 fans work abnormally. The abnormal fan number is behind Num. For example, Num 3 5.

     14:55:08 08/14/2008 UTC alarm 80 occurred Fan error, reason: Current Trunk Bottom Fan Num 3 4 7 8 fail to work sent by UPC(MPU) 1

  iv. Current Cabinet Top Fan Num …..fail to work

     One or two of the 6 fans work abnormally. The abnormal fan number is behind Num. For example, Num 3 5.

     14:57:38 08/14/2008 UTC alarm 80 occurred Fan error, reason: Current Cabinet Top Fan Num 3 4 fail to work sent by UPC(MPU) 1

- Corrent alarm(Both old and new racks can generate this alarm) is as follows:

  i. Fan recover: Current Cabinet/Trunk Fan work normal

  14:58:38 08/14/2008 UTC alarm 80 cleared Fan recorver: Current Cabinet/Trunk Fan work normal sent by UPC(MPU) 1

Alarm Description Fan malfunction.

Supported Devices T128/T64,T600/T1200

Appendix Specification T64, T128 adopts old rack; T600, T1200 adopts new rack.

Board Alarms

279

Message No. 279

Default Severity Level 3

Cause The line board is offline.

Recommended Operations Check whether the line board is unplugged normally, or the board offline is caused by abnormal line card.

293

Message No. 293

Default Severity Level 3

Cause When the active board and standby board change over, the Card Type reported by the lower layer BSP is not in the valid range. Its value is abnormity.

Recommended Operations This alarm is used for the location of the malfuction. It has no influence on the operation or the utility.

299

Message No. 299

Default Severity Level 3

Alarm Recovery Available

Alarm Type Equipment Alarm

NM Level 2

Cause Alarm occurs:

Device is removed from 59 stack system.

	Alarm clears: Device is added to 59 stack system.
Related Alarms	512, 18720, 18721.
Recommended Operations	Check whether any device is removed from stack system.
Alarm Prototype Description	Alarm occurred Remove Device No.%d! (%d is device number) Alarm cleared Add Device No.%d! (%d is device number) Example: 15:50:49 01/22/2008 UTC alarm 299 cleared %Board% Add Device No.3! sent by Stack Master DevId 2 15:52:13 01/22/2008 UTC alarm 299 occurred %Board% Remove Device No.3! sent by Stack Master DevId 2
Alarm Description	Device is removed from stack system.
Supported Devices	59 stack system.
Appendix Specification	N.A.

300

Message No.	300
Default Severity Level	2
Alarm Recovery	Available
Alarm Type	Equipment Alarm
NM Level	1
Cause	The double **SFC**(**MPU, RPU**) are both active or both standby caused by hardware malfunction.
Influence	The rack can not work normally.
Related Alarms	No.
Recommended Operations	1. Reboot the two boards with abnormal alarm. 2. If reboot operation is invalid, contact with ZTE service staff. 3. ZTE service staff can input printHardwareState in ros and record the result.
Alarm Prototype Description	2 %s is %s,system abnormal. The first %s is the abnormal CPU type. Generally it is SFC, MPU or RPU. The second %s is the abnormal master or slave state. The second %s is the abnormal master or slave state. 16:30:38 06/21/2007 UTC alarm 300 occurred 2 SFC is master,system abnormal. sent by UPC(MPU) 2 16:38:39 06/21/2007 UTC alarm 300 cleared 2 SFC is master,system abnormal. sent by UPC(MPU) 2
Alarm Description	The double SFC (MPU, RPU) are both active or both standby caused by hardware malfunction.

Supported Devices	T64/T1200, T600/T1200.
Appendix Specification	N.A.

301

Message No.	301
Default Severity Level	6
Alarm Recovery	Unavailable
Alarm Type	Equipment Alarm
NM Level	5
Cause	Abnormality of NPCT line card will lead to interruption of switch network reset, which further causes the repeat reset of switch network and thus normal line cards in other slots will fail to send packets normally. To solve this problem, we give a limit to reset times. If the times of switch network reset caused by abnormal line card exceed this threshold, only alarm will be prompted and switch network will not be reset.
Influence	The linecard with malfunction can not work normally. There is no influence on other linecards.
Related Alarms	No.
Recommended Operations	Wait for engineer from customer service department to deal with the fault line card.
Alarm Prototype Description	Pannel %d NPC resets switch module over limit times %d line card slot number 11:02:34 03/21/2008 UTC alarm 301 occurred Pannel 5 npc resets switch module over limit times. sent by UPC(MPU) 1
Alarm Description	The times of SFU reset caused by abnormal line card exceed this threshold.
Supported Devices	T64E/T128
Appendix Specification	N.A.

302

Message No.	302
Default Severity Level	6
Alarm Recovery	Unavailable
Alarm Type	Equipment Alarm
NM Level	5
Cause	Abnormality of **NPCT** line card will lead to failure of **SFC** synchronization. In case synchronization loss still exists for switch chip on **SFC** after it resets repeatedly for 30 times, master/slave switchover of **SFC** will occur and alarm is sent out.

	To avoid continuous switchover of master/slave **SFC**, we set a limit to the switchover. When threshold is exceeded, master/slave switchover of **SFC** will stop.
Influence	The linecard with malfunction leads to the active/standby switchover.
Related Alarms	294, alarm generated by line card out of synchronism.
Recommended Operations	No.
Alarm Prototype Description	Pannel %d SFC is exchanged to be slave because switch-module is unsynchronous. %d: SFC slot number 11:15:57 03/21/2008 UTC alarm 302 occurred Pannel 1 SFC is exchanged to be slave because switch-module is unsynchronous. sent by UPC(MPU) 1
Alarm Description	SFC synchronization fails. Master/slave switchover of SFC will occur and alarm is sent out
Supported Devices	T64E/T128
Appendix Specification	N.A.

303

Message No.	303
Default Severity Level	6
Alarm Recovery	Unavailable
Alarm Type	Equipment Alarm
NM Level	5
Cause	It fails to read/write card memory due to the problem of hardware.
Influence	The single board can not work normally. The thread application on the single board may suspend due to the abnormal memory
Related Alarms	No.
Recommended Operations	Wait for engineer from customer service department to deal with the fault line card
Alarm Prototype Description	Pannel:%d NPC %s data eye abnormal. %d line card slot number %s Master/slave, Master/slave line card 13:31:30 03/25/2008 UTC alarm 303 occurred Pannel:7 NPC master data eye abnormal. sent by UPC(MPU) 1
Alarm Description	The thread application on the single board may suspend due to the abnormal memory read-write.
Supported Devices	T64E/T128, T1200

Appendix Specification	N.A

310

Message No.	310
Default Severity Level	6
Alarm Recovery	Unavailable
Alarm Type	Equipment Alarm
NM Level	5
Cause	The hardware is instable. Fails to write to the register in interface board initialization or the platform command configuration.
Influence	The interface board or the line card can not work normally. The platform command configuration fails.
Related Alarms	No.
Recommended Operations	Plug the interface board or the line card again. If the malfunction still exists, then contact ZTE customer service personnel to check whether the interface board or the line card is abnormal.
Alarm Prototype Description	write register failed:baseaddr = 0x%08x ,offset =0x%4x %08x: the base address %04x: the offset address Example: 14:17:56 05/20/2008 UTC alarm 303 occurred %Board% write register failed:baseaddr = 0xC6002000 ,offset =0x0006 sent by NPC 2
Alarm Description	Alarm appears when the line card fails to modify the register. Alarm may also appear when failing to write to the register in interface board initialization or the platform command configuration. It is used to diagnose the hardware abnormity.
Supported Devices	T64E/T128, T600/T1200
Appendix Specification	N.A

311

Message No.	311
Default Severity Level	5
Alarm Recovery	Unavailable
Alarm Type	Equipment Alarm
NM Level	5
Cause	The board link forwarding is abnormal.
Influence	The corresponding hardware reboots.
Related Alarms	No.

Recommended Operations	Check whether the board link forwarding is normal; whether the hardware works normally.
Alarm Prototype Description	Alarm occurred NP %d link exception cause %s %s,warning; %d: board number The first %s is the hardware name: 870874FPGASFCBOARD. The second %s is the action: reset, rotate Example: 15:29:12 08/09/2008 UTC alarm 311 occurred %Board% link exception cause 874 reset,warning sent by NPC 9 15:28:29 08/09/2008 UTC alarm 311 occurred %Board% link exception cause two 870 reset,warning sent by NPC 9 15:29:30 08/09/2008 UTC alarm 311 occurred %Board% link exception cause FPGA reset,warning sent by NPC 9 15:44:23 08/09/2008 UTC alarm 311 occurred %Board% link exception cause SFC rotate,warning sent by NPC 9 15:46:16 08/09/2008 UTC alarm 311 occurred %Board% link exception cause board reset,warning sent by NPC 9
Alarm Description	The board link forwarding is abnormal which brings to something wrong in the corresponding hardware
Supported Devices	T64E/T128, T600/T1200
Appendix Specification	N.A.

312

Message No.	312
Default Severity Level	5
Alarm Recovery	Available
Alarm Type	Equipment Alarm
NM Level	2
Cause	Alarm occurred The board link forwarding is abnormal. User configuration interface is down physically. Alarm cleared The board link forwarding works normally for the specified time. User configuration interface is up physically.
Influence	User configuration interface is up/down.
Related Alarms	512
Recommended Operations	Check whether the board link forwarding is normal; whether the user configures this interface.

Alarm Prototype Description	NP %d link exception cause interface %s %s,warning %d: board number The first %s is the interface name. The second %s means that the interface is enabled or disabled. Alarm occurred: shutdown Alarm cleared: up Example: 15:30:31 08/09/2008 UTC alarm 312 occurred %Board% link exception cause interface fei_9/5 shut down,warning sent by NPC 9 16:36:27 08/09/2008 UTC alarm 312 cleared %Board% link exception cause interface fei_9/5 up,warning sent by NPC 9
Alarm Description	The board link forwarding is abnormal which brings to the user configuration interface down.
Supported Devices	T64E/T128, T600/T1200
Appendix Specification	N.A

313

Message No.	313
Default Severity Level	6
Alarm Recovery	Unavailable
Alarm Type	Equipment Alarm
NM Level	2
Cause	The forwading link on np is always abnormal and can not be solved.
Influence	Discard the packets and take corresponding actions.
Related Alarms	311
Recommended Operations	Check whether the board link forwarding is normal or not. Whether there is packet loss or not. The device reboots the relative hardware automatically.
Alarm Prototype Description	NP %d forward link has exception,warning %d: board number 15:27:36 08/09/2008 UTC alarm 313 occurred %Board% NP 6 forward link has exception,warning sent by NPC 6
Alarm Description	The forwarding link is abnormal.
Supported Devices	T64E/T128, T600/T1200

Appendix Specification N.A.

Port Alarm

512

Message No. 512

Default Severity Level 6

Cause The port is down or up.

Recommended Operations If it is a port down message, please check whether the port connection is normal.

Alarm Prototype Description Alarm occurs:

10:12:57 09/15/2003 UTC alarm 512 occurred. %PORT% Port Down on fei_5/6 sent by SMP 1

Alarm clears:

10:12:59 09/15/2003 UTC alarm 512 cleared. %PORT% Port Up on fei_5/6 sent by SMP 1

540

Message No. 540

Default Severity Level 6

Cause The aggregation of port configuration in SMARTGROUP interface is successful.

Recommended Operations No.

541

Message No. 541

Default Severity Level 6

Cause The aggregation of port configuration in SMARTGROUP interface fails.

Recommended Operations No.

542

Message No. 542

Default Severity Level 6

Cause For a certain interface board, the quantity of local port returned from lower layer is 0.

Recommended Operations No.

Software Alarm

ETHOAM Alarm

16128

Message No. 16128

Default Security Level 5

Alarm Type "ProcessingErrorAlarm"

NM Level 5

Cause The local end starts loopback and the remote end fails to respond for the reason that the response is delayed or the status configuration is not correct.

Influence Loopback fails.

Recommended Operations Start loopback again.

Alarm Description Prototype Interface %s

%s is the reason.

The details are as follows:

1. loopback failure for Mode

   Ethernet oam protocol mode can’t satisfy loopback sending condition.

2. Ethernet oam is not enable

   Ethernet oam is not enabled.

3. Discovery is undone

   Ethernet oam protocol negotiation fails.

4. in slave mode

   Local end ethernet oam is in slave mode.

5. loopback has on/off

   Local end ethernet oam is in on/off mode.

6. loopback respond start command failed

   Remote respond loopback start fails.

7. loopback respond stop command failed

Remote respond loopback stop fails.

Examples:

00:16:14 01/01/2001 UTC alarm 16128 occurred %ETHOAM% Interface loopback respond start command failed on fei_1/1 sent by NPC 1

00:16:14 01/01/2001 UTC alarm 16128 occurred %ETHOAM% Interface loopback respond stop command failed on fei_1/1 sent by NPC 1

Alarm Description The local end starts loopback and the remote end fails to respond.

Supported Devices All series (This alarm can be available from V4.8.22.)

16129

Message No. 16129

Default Security Level 5

Alarm Type "CommunicationAlarm"

NM Level 5

Cause Lost the message that keeps protocol success status within timer time.

Influence Cause local Ethernet oam protocol status initialization.

Recommended Operations Check if link and packet sending/receiving in receive direction are normal and re-initiate protocol negotiation.

Alarm Description Prototype Interface %s localmac %s peermac %s

The first %slost link in receive direction.

The second %s and the third %ssource MAC address and destination MAC address.

Examples:

00:16:14 01/01/2001 UTC alarm 16129 occurred %ETHOAM% Interface lost ink in receive direction localmac 00d0.d0c6.5e27 peermac 00d0.d0c0.7d81 on fei_1/1 sent by NPC 11

Alarm Description Packets fail to be received on receive direction of link.

Supported Devices All series (This alarm can be available from V4.8.22.)

16130

Message No. 16130

Default Security Level 5

Alarm Type "ProcessingErrorAlarm"

NM Level 5

Cause The local or remote configuration modification causes that the local or remote can’t satisfy the modified configuration.

Influence Cause Ethernet oam protocol status to change.

Recommended Operations	Check attribute configuration and re-initiate Ethernet OAM protocol negotiation.
Alarm Description Prototype	Discovery %s localmac %s peermac %s The first %s details are as follows: 1. Reset for remote unsatisfied The remote can't satisfy the modified configuration. 2. Reset for local unsatisfied The local can't satisfy the modified configuration. 3. is successfully connected Discovery is successfully connected. The second %s and the third %s: source MAC address and destination MAC address. Examples: 00:16:14 01/01/2001 UTC alarm 16130 occurred %ETHOAM% Discovery Reset for remote unsatisfied localmac 00d0.d0c6.5e27 peermac 00d0.d0c0.7d81 on fei_1/1 sent by NPC 1 00:16:14 01/01/2001 UTC alarm 16130 occurred %ETHOAM% Discovery Reset for local unsatisfied localmac 00d0.d0c6.5e27 peermac 00d0.d0c0.7d81 on fei_1/1 sent by NPC 1 00:16:14 01/01/2001 UTC alarm 16130 occurred %ETHOAM% Discovery is successfully connected localmac 00d0.d0c6.5e27 peermac 00d0.d0c0.7d81 on fei_1/1 sent by NPC 1
Alarm Description	The local and remote can't satisfy the Ethernet oam protocol attribute configuration..
Supported Devices	All series (This alarm can be available from V4.8.22.)

16131

Message No.	16131
Default Security Level	5
Alarm Type	"CommunicationAlarm"
NM Level	5
Cause	The local receives the related fault event such as link fault, dying gasp fault and fault frame event.
Influence	Generate protocol message to inform remote related event and print alarm locally.
Recommended Operations	Check attribute configuration and re-initiate Ethernet OAM protocol negotiation.
Alarm Description Prototype	Discovery %s localmac %s peermac %s The first %s details are as follows: 1. Link fault: check link state 2. Dying gasp fault: check device state 3. Critical fault: check device state 4. Error frame event: check received error frames

Alarm Description

Interface %s localmac %s peermac %s

The first %s details are as follows:

1. occur remote link fault

   occur remote link fault event
2. occur remote dying gasp event

   occur remote dying gasp event
3. occur remote critical event

   occur remote critical event
4. occur local link fault

   occur local link fault
5. occur local dying gasp event

   occur local dying gasp event
6. occur local critical event

   occur local critical event
7.
   i. occur error frame event

      occur error frame event locally
   ii. occur error frame-period event

      occur error frame-period event locally
   iii. occur error frame-second event

      occur error frame-second event locally
   iv. occur error symbol-period event

      occur error symbol-period event locally

The second %s and the third %s: source MAC address and destination MAC address

Example:

1. 00:16:14 01/01/2001 UTC alarm 16131 occurred %ETHOAM% Interface occur remote link fault localmac 00d0.d0c6.5e27 peermac 00d0.d0c0.7d81 on fei_1/1 sent by NPC 1
2. 00:16:14 01/01/2001 UTC alarm 16131 occurred %ETHOAM% Interface occur remote dying gasp event localmac 00d0.d0c6.5e27 peermac 00d0.d0c0.7d81 on fei_1/1 sent by NPC 1
3. 00:16:14 01/01/2001 UTC alarm 16131 occurred %ETHOAM% Interface occur remote critical event localmac 00d0.d0c6.5e27 peermac 00d0.d0c0.7d81 on fei_1/1 sent by NPC 1
4. 00:16:14 01/01/2001 UTC alarm 16131 occurred %ETHOAM% Interface occur local link fault localmac 00d0.d0c6.5e27 peermac 00d0.d0c0.7d81 on fei_1/1 sent by NPC 1
5. 00:16:14 01/01/2001 UTC alarm 16131 occurred %ETHOAM% Interface occur local dying gasp event localmac 00d0.d0c6.5e27 peermac 00d0.d0c0.7d81 on fei_1/1 sent by NPC1
6. 00:16:14 01/01/2001 UTC alarm 16131 occurred %ETHOAM% Interface occur local critical event localmac 00d0.d0c6.5e27 peermac 00d0.d0c0.7d81 on fei_1/1 sent by NPC1

7. 00:16:14 01/01/2001 UTC alarm 16131 occurred %ETHOAM% Interface occur error frame event localmac 00d0.d0c6.5e27 peermac 00d0.d0c0.7d81 on fei_1/1 sent by NPC 1
8. 00:16:14 01/01/2001 UTC alarm 16131 occurred %ETHOAM% Interface occur error frameperiod event localmac 00d0.d0c6.5e27 peermac 00d0.d0c0.7d81 on fei_1/1 sent by NPC 1
9. 00:16:14 01/01/2001 UTC alarm 16131 occurred %ETHOAM% Interface occur error framesecond event localmac 00d0.d0c6.5e27 peermac 00d0.d0c0.7d81 on fei_1/1 sent by NPC 1
10. 00:16:14 01/01/2001 UTC alarm 16131 occurred %ETHOAM% Interface occur error symbol- period event localmac 00d0.d0c6.5e27 peermac 00d0.d0c0.7d81 on fei_1/1 sent by NPC 1

Alarm Description The device occurs related fault event such as link fault, dying gasp fault and fault frame event.

Supported Devices All series (This alarm can be available from V4.8.22.)

30464

Message No. 30464

Default Security Level 6

Alarm Recovery Available

Alarm Type "ProcessingErrorAlarm"

NM Level 5

Cause Local configuration has fault. The peer receives faulty CC message or doesn't receive CC message that local sends.

Influence Local prints alarm.

Recommended Operations Link fault: check link state, check configuration.

Alarm Description Prototype %s MD %d MA %d MEP %d, %s

The first %d is

the ID of MD with RDI alarm.

The second %d is

the ID of MA with RDI alarm.

The third %d is

the ID of MEP with RDI alarm.

The first %s is

someRDIdefect,

when alarm appears, the alarm is the content which shows.

When alarm disappears, this character string is empty.

The second character string content is

has received a packet from some remote MEPs with RDI flag!

when alarm appears, the alarm is the content which shows above.

all remote MEPs RDI defect disappear!

when alarm disappears, the alarm is the content which shows above.

Example:

1. 10:38:07 08/10/2009 UTC alarm 30464 occurred %CFM% MD 1 MA 1 MEP 2,has received a packet from some remote MEPs with RDI flag
2. 10:38:10 08/10/2009 UTC alarm 30464 occurred %CFM% MD 1 MA 1 MEP 2, all remote MEPs RDI defect disappear!

Alarm Description When CC message that sends from peer has RDI, this alarm appears.

Supported Devices All series

Appendix Specification This alarm can be available from V4.8.23.

30465

Message No. 30465

Default Security Level 6

Alarm Recovery Available

Alarm Type Communication Alarm

NM Level 5

Cause Local can't receive CC message of peer.

Influence This leads to protocol message to inform remote related event and local printing alarm.

Recommended Operations Link fault: check link state, check configuration.

Alarm Description Prototype SomeRMEPCCMdefect,MD %d MA %d MEP %d , s

The first %d is

the ID of MD with DefRemoteCCM alarm.

The second %d is

the ID of MA with DefRemoteCCM alarm.

The third %d is

the ID of MEP with DefRemoteCCM alarm.

The first %s is

has not received CCM from some remote MEPs expired 3.5 times CCM's transmission interva

when alarm appears, the alarm is the content which shows above.

SomeRMEPCCMdefect defect disappear!

when alarm disappears, the alarm is the content which shows above.

Example:

1. 10:38:07 08/10/2009 UTC alarm 30465 occurred %CFM% SomeRMEPCCMdefect,MD 1 MA 1 MEP 2,has not received CCM

from some remote MEPs expired 3.5 times CCM's transmission interval!

2. 10:38:10 08/10/2009 UTC alarm 30465 occurred %CFM% MD 1 MA 1 MEP 2, SomeRMEPCCMdefect defect disappear!

Alarm Description When configured local MEP can't receive CC message sended from peer, this alarm will appaer.

Supported Devices All series

Appendix Specification This alarm can be available from V4.8.23.

30466

Message No. 30466

Default Security Level 6

Alarm Recovery Available

Alarm Type ConfigureErrorAlarm

NM Level 5

Cause The local or peer configuration has error. Local receives faulty CC message.

Influence Local prints alarm.

Recommended Operations View local and remote configurations.

Alarm Description Prototype %s MD %d MA %d MEP %d, %s

The first %d is

the ID of MD with RDI alarm.

The second %d is

the ID of MA with RDI alarm.

The third %d is

the ID of MEP with ERR alarm.

The first %s is

errorCCMdefect, .

when alarm appears, the alarm is the content which shows above.

When alarm disappears, this character string is empty.

The second character string content is

one or more invalid CCMs has been received!

when alarm appears, the alarm is the content which shows above.

errorCCMdefect defect disappear!

when alarm disappears, the alarm is the content which shows above.

Example:

1. 10:38:07 08/10/2009 UTC alarm 30466 occurred %CFM% MD 1 MA 1 MEP 2, one or more invalid CCMs has been received!

2. 10:38:10 08/10/2009 UTC alarm 30466 occurred %CFM% MD 1 MA 1 MEP 2, errorCCMdefect defect disappear!

Alarm Description When local receives faulty CC message that sends from peer, this alarm appears.

Supported Devices All series

Appendix Specification This alarm can be available from V4.8.23.

30467

Message No. 30467

Default Security Level 6

Alarm Recovery Available

Alarm Type ConfigureErrorAlarm

NM Level 5

Cause Receive the CC messge which doesn't belong to this Level or doesn't belong to this MA.

Influence Local prints alarm.

Recommended Operations View local and remote configurations.

Alarm Description Prototype %s MD %d MA %d MEP %d, %s

The first %d is

the ID of MD with RDI alarm.

The second %d is

the ID of MA with RDI alarm.

The third %d is

the ID of MEP with XCON alarm.

The first %s is

xconCCMdefect,

when alarm appears, the alarm is the content which shows above.

When alarm disappears, this character string is empty.

The second character string content is

one or more cross connect CCMs has been received!,

when alarm appears, the alarm is the content which shows above.

xconCCMdefect defect disappear!

when alarm disappears, the alarm is the content which shows above.

Example:

1. 10:38:07 08/10/2009 UTC alarm 30467 occurred %CFM% MD 1 MA 1 MEP 2, one or more cross connect CCMs has been received!
2. 10:38:10 08/10/2009 UTC alarm 30467 occurred %CFM% MD 1 MA 1 MEP 2, xconCCMdefect defect disappear!

Alarm Description When the CC messge which doesn't belong to this Level or this MA is received, this alarm appears.

Supported Devices All series

Appendix Specification This alarm can be available from V4.8.23.

ROS Alarm

16384

Message No. 16384

Cause The process is suspended.

Recommended Operations Please copy and save the information, then contact ZTE maintenance staff.

16386

Message No. 16386

Cause Privileged mode password is changed.

Recommended Operations Please check the password.

16389

Message No. 16389

Default Severity Level 6

Cause The rack is cold starting which is opposite to hot starting. Cold starting means that to turn on the power and start-up the device. Hot starting means that to reboot the device when it is still running.

Recommended Operations No.

Alarm Prototype Description Alarm occurred

11:22:27 05/29/2007 UTC alarm 16389 occurred %ROS% SNMP agent on host ZTE is undergoing a cold start sent by MCP

16391

Message No. 16391

Default Severity Level 5

Alarm Recovery Unavailable

Alarm Type CLASS_NOTIFY

NM Level 4

Cause	The current version is in trial run state.
Recommended Operations	The command updatever activate in privilege mode can be used to remove the try-running alarm.
Alarm Prototype Description	Current version is in try-running and activate it please. Example: 14:28:01 03/21/2008 UTC alarm 16392 occurred %ROS% Current version is in try-running and please activate it sent by MEC 1.
Alarm Description	The current version is in trial running state and it need to be activated by users. Or the device reboots automatically after a while. The remaining time can be viewd by command **show updatever** in privileged mode.
Supported Devices	CE&PTN 6100 CE&PTN 8900
Appendix Specification	CE&PTN version supports this alarm.

16392

Message No.	16392
Default Severity Level	5
Alarm Type	CLASS_NOTIFY
NM Level	4
Cause	The current version is the rollback. The reason may be that the trial run fails when updating the version.
Recommended Operations	The command updatever activate in privilege mode can be used to remove the trial run alarm.
Alarm Prototype Description	Back-version is running now for loading update-version failed 14:27:32 03/21/2008 UTC alarm 16392 occurred %ROS% Back-version is running now for loading update-version failed sent by MEC 1
Alarm Description	The current version is the rollback. The reason may be that the trial run fails when updating the version
Supported Devices	CE&PTN 6100 CE&PTN 6100
Appendix Specification	CE &PTN version supports this alarm.

16393

Message No.	16393
Default Severity Level	5
Alarm Recovery	Unavailable
Alarm Type	CLASS_NOTIFY
NM Level	5

Cause	A prompt appears: succeed to download and upgrade the version, but fail to write the upgrade rollback.
Recommended Operations	No.
Alarm Prototype Description	Downloading update-version file successfully but setting the flag failed Example: 14:29:01 03/21/2008 UTC alarm 16392 occurred %ROS% Downloading update-version file successfully but setting the flag failed sent by MEC 1
Alarm Description	A prompt appears: succeed to download and upgrade the version, but fail to write the upgrade rollback.
Supported Devices	CE&PTN 6100 CE&PTN 8900
Appendix Specification	CE&PTN version supports this alarm.

16394

Message No.	16394
Default Severity Level	5
Alarm Recovery	Available
Alarm Type	Equipment Alarm
NM Level	5
Cause	Alarm occurred Users configure the device again after plugging the backplane. The backplan backup does not complete. Alarm cleared The backplane finishes the backup for the main board. The backplane can work instead of the main board.
Influence	The backplane can not work instead of the main board.
Recommended Operations	Wait for a while to see whether the alarm recovers. Or check whether the backplane backup the data on the main board.
Alarm Prototype Description	Alarm occurred Slave is not a copy of master. Slave board can not substitute for master board. 14:50:22 08/20/2008 green alarm 16394 occurred %ROS% Slave is copying of master. Slave board can not substitute for master board. sent by UPC(MPU) 2 Alarm cleared Slave is a copy of master. Slave board can substitute for master board. 14:59:17 08/20/2008 green alarm 16394 cleared %ROS% Slave is a copy of master. Slave board can substitute for master board. sent by UPC(MPU) 2.

Alarm Description	The backplan backup does not complete. It can not work instead of the main board.
Supported Devices	T64E/T128

16395

Message No.	16395
Default Security Level	5
Alarm Recovery	Available
Alarm Type	"EquipmentAlarm"
NM Level	4
Cause	SD is removed.
Influence	SD removed notice
Recommended Operations	Insert SD
Alarm Description Prototype	Alarm Occured SD is removed Slave SD is removedslave board Alarm Recovery SD is inserted Slave SD is insertedslave board Examples: Alarm Occured 18:30:50 09/02/2008 alarm 16395 occurred %ROS% SD is removed sent by MEC 1 18:32:55 09/02/2008 alarm 16395 occurred %ROS% Slave SD is removed sent by MEC2 Alarm Recovery 18:30:51 09/02/2008 alarm 16395 cleared %ROS% SD is inserted sent by MEC 1 18:33:00 09/02/2008 alarm 16395 cleared %ROS% Slave SD is inserted sent by MEC2
Alarm Description	SD is removed.
Supported Devices	89 and 69 series routing switch(This alarm can be available from V4.8.22.)

16396

Message No.	16396
Default Security Level	4
Alarm Type	"ProcessingErrorAlarm"

NM Level	5
Cause	When slice memory is applied, if the first valid slice memory in slice idle table, the physical next block or the logical next block has check failure the applied slice memory is modified illegally.
Influence	Maybe memory is exhausted.
Recommended Operations	Use the **show processor** command to view if memory utilization Memory is abnormal.
Alarm Description Prototype	Slice Isolate Unit(%d) Times(%d) At Tick(%d) On %s(%s) Panel(%d)! The first %d: slice memory queue type, the range is from 2 to 30. The second %d: isolated times, the maximum is 256. The third %d: tick value in this isolation. The first %ssingle board type, the value is RP,MP,SP or NP. The second %s: single board master/slave type, master is M , slave is S. The fourth %dpanel number of single board. Example: 18:28:05 10/17/2008 UTC alarm 16396 occurred %ROS% Slice Isolate Unit(3) Times(1) At Tick(15628) On RP(M) Panel(1)! sent by UPC(RPU) 1
Alarm Description	Slice memory check fails.
Supported Devices	T128/T600/T1200 device (This alarm can be available from V4.8.20.)

DATABASE Alarm

16640

Message No.	16640
Default Severity Level	3
Cause	Database writing is wrong.
Recommended Operations	Check whether the system is running normally. If it occurrs in system configuration, it may try again a few minutes later.

16642

Message No.	16642
Default Severity Level	6
Cause	The alarm buffer only has 20% space left.
Recommended Operations	If it does not configure to send alarm messages to external server in ftp or syslog mode, please check if there is any important alarm

message in alarm buffer by using **show logging alarm** command; if there is, copy the important alarm message for backup. Set alarm log buffer size by using command **logging buffer** <*buffer -size*>."buffer-size" is the size of alarm buffer: 100~1000, 200K by default.

16643

Message No. 16643

Default Severity Level 5

Cause The alarm buffer overflows. Some old alarm messages will be cleared.

Recommended Operations If alarm message is needed, export alarm message at first. Set alarm log buffer size by using command **logging buffer** <*buffer-size*>. "buffer-size" is the size of alarm buffer: 100~1000, 200K by default.

16644

Message No. 16644

Default Severity Level 3

Cause The alarm buffer overflows. Some old alarm messages will be cleared.

Recommended Operations If alarm message is needed, export alarm message at first. Set alarm log buffer size by using command **logging buffer** <*buffer-size*>. "buffer-size" is the size of alarm buffer: 100~1000, 200K by default.

16645

Message No. 16645

Default Severity Level 3

Cause The standby board fails to acquire the main board database file via FTP.

Recommended Operations Check the system running status. Restart the standby board if necessary.

16646

Message No. 16646

Default Severity Level 3

Cause The node recursion level is too deep in the program to delete the database.

Recommended Operations	There may be redundant configuration. Please contact ZTE for the solution.

OAM Alarm

16899

Message No.	16899
Default Severity Level	5
Alarm Recovery	Available
Alarm Type	QoSAlarm
NM Level	4
Cause	CPU load, namely CPU utilization ratio reaches the set low threshold.
Influence	It may bring to the slow operation response.
Related Alarms	16900, 16901
Recommended Operations	If the operation with great consumption on cpu is carried out in short time, then it is normal phenomenon. Commands show process, show process detail can be used to view CPU utilization.
Alarm Prototype Description	%s(M) panel %d current CPU load is: %d% %s(S) panel %d current CPU load is: %d% The first %s is the CPU type. The first %d is panel number and the second %d is CPU utilization. Alarm occured: An alarm 16899 level 5 occurred at 00:52:07 01/01/2001 UTC sent by UPC(MPU) 1 %OAM% CPU load exceeds the lowest threshold NP(M) panel 7 current CPU load is: 80%. Alarm cleared: An alarm 16899 level 5 cleared at 00:53:07 01/01/2001 UTC sent by UPC(MPU) 1 %OAM% CPU load exceeds the lowest threshold NP(M) panel 7 current CPU load is: 50%.
Alarm Description	CPU load, namely CPU utilization ratio exceeds the set low threshold.
Supported Devices	All.
Appendix Specification	The platform 4.6.03b and the upgrade versions support this alarm. Not CE&PTN version.

16900

Message No.	16900
Default Severity Level	5

Alarm Recovery	Available
Alarm Type	QoSAlarm
NM Level	4
Cause	CPU load, namely CPU utilization ratio reaches the set middle threshold.
Influence	It may bring to the slow operation response.
Related Alarms	16899, 16901
Recommended Operations	If the operation with great consumption on cpu is carried out in short time, then it is normal phenomenon. Commands show process, show process detail can be used to view CPU utilization.
Alarm Prototype Description	%s(M) panel %d current CPU load is: %d% %s(S) panel %d current CPU load is: %d% The first %s is CPU type. The first %d is panel number and the second %d is CPU utilization.
Alarm Description	CPU load, namely CPU utilization ratio exceeds the set middle threshold.
Supported Devices	All.
Appendix Specification	The platform 4.6.03b and the upgrade versions support this alarm. Not CE&PTN version.

16901

Message No.	16901
Default Severity Level	5
Alarm Recovery	Available
Alarm Type	QoSAlarm
NM Level	3
Cause	CPU load, namely CPU utilization ratio reaches the set high threshold.
Influence	It may bring to the slow operation response.
Related Alarms	16899, 16900
Recommended Operations	If the operation with great consumption on cpu is carried out in short time, then it is normal phenomenon. Commands show process, show process detail can be used to view CPU utilization.
Alarm Prototype Description	%s(M) panel %d current CPU load is: %d% %s(S) panel %d current CPU load is: %d% The first %s is CPU type. The first %d is panel number and the second %d is CPU utilization.
Alarm Description	CPU load, namely CPU utilization ratio exceeds the set high threshold.
Supported Devices	All.
Appendix Specification	The platform 4.6.03b and the upgrade versions support this alarm. Not CE&PTN version.

16903

Message No. 16903

Default Severity Level 5

Cause FLASH tests are not successful.

Recommended Operations Check the hardware of the equipment and check whether FLASH exists or there is something abnormal.

16904

Message No. 16904

Default Severity Level 5

Cause FLASH exists but can not work normally after setting up the rack.

Recommended Operations Change FLASH for a new one, or set up the rack without FLASH.

16905

Message No. 16905

Default Severity Level 4

Cause Backplane fails to write nvram.

Recommended Operations Backup the configuration to prevent configuration loss. Check whether the backplane is running normally. Change the backplane if neccesarry.

16906

Message No. 16906

Default Severity Level 6

Cause Distributing system RP sends a message to MP and inform to add or delete interface. Give an alarm after the synchronized message fails.

Recommended Operations Send the alarm message to ZTE's maintenance personnel.

16907

Message No. 16907

Default Severity Level 5

Cause When QoS is applied for dynamic memory, the application fails.

Recommended Operations Send the alarm message to ZTE's maintenance personnel.

16916

Message No. 16916

Default Severity Level 6

Cause The ftp user logs into the device.

Recommended Operations No.

Alarm Prototype Description Alarm occurred

00:02:21 01/01/2001 UTC alarm 16916 occurred %OAM% ftp user from 192.168.1.125 port: 3549 to loacl:192.168.1.10 port:21IN OK sent by MCP

16917

Message No. 16917

Default Severity Level 5

Cause If one of the terminal executes "write" operation, then the terminal is still in the phase of configure collection. If the connection is cut down for some reason, then the alarm is generated. The possibility of disconnection is as follows:

- Console, telnet connection times out.
- Other terminal execute **clear tcp** to delete a TCP link.

Recommended Operations Please do not cut down the connection when the "write" operation is being performed. If the terminal connection is cut down in the phase of configure collection, then all the write operations are stopped.

Alarm Prototype Description Alarm occurred

The serial port interrupts to execute write.

10:52:25 06/27/2007 UTC alarm 16917 occurred %OAM% Writing configuration aborted because con 0 is closed! sent by UPC(MPU) 1!

Telnet execute write terminal:

10:56:20 06/27/2007 UTC alarm 16917 occurred %OAM% Writing configuration aborted because vty 0 is closed! sent by UPC(MPU) 1

The terminal number after vty keeps consistent with the one after command **who**.

16918

Message No. 16918

Default Severity Level	5
Cause	If one of the terminal execute "write" operation, then the terminal is in the phase of background file copy because it already finishes the configure collection, if the connection is cut, then alarm is generated. The possibility of disconnection is as follows: ■ Cut down the windows of the terminal directly. ■ Console, telnet connection times out. ■ Other terminal executes **clear tcp** to delete a TCP link.
Recommended Operations	Do not cut this connection as much as possible when "write" operation is being performed. If connection is cut down when write is still executing file operation, then "write" continues in the background as far as the final "startrun" created. Please do not restart the bracket.
Alarm Prototype Description	Alarm occurred The serial port interrupts to execute write. 10:59:29 06/27/2007 UTC alarm 16918 occurred %OAM% Con 0 is closed, but writing configuration is still in process! sent by UPC(MPU) 1 Telnet executes write terminal: 10:59:29 06/27/2007 UTC alarm 16918 occurred %OAM% Vty 1 is closed, but writing configuration is still in process! sent by UPC(MPU) 1 The terminal number after vty keeps consistent with the one after command **who**.
Appendix Specification	Please do not restart the rack in order to prevent the created "startrun" not complete. Reboot operation may lead to the loss of rack configuration or the command line error. Use dir to confirm whether startrun file is updated.

16919

Message No.	16919
Default Severity Level	6
Cause	FTP users delete the files on the device.
Alarm Prototype Description	Alarm occurred 00:07:21 01/01/2001 UTC alarm 16919 occurred %OAM% DELE file /flash/1.txt sent by MCP
Appendix Specification	Please do not restart the rack in order to prevent the created "startrun" not complete. Reboot operation may lead to the loss of rack configuration or the command line error. Use dir to confirm whether startrun file is updated.

16920

Message No.	16920

Default Severity Level	6
Cause	The ftp user uplosds files to the device.
Alarm Prototype Description	Alarm occurred 00:05:49 01/01/2001 UTC alarm 16920 occurred %OAM% STOR file /flash/1.txt sent by MCP

16921

Message No.	16921
Default Severity Level	6
Cause	The ftp user copies files on the device.
Alarm Prototype Description	Alarm occurred 00:04:25 01/01/2001 UTC alarm 16921 occurred %OAM% RETR file /flash/hes59.bin sent by MCP

16922

Message No.	16922
Default Severity Level	6
Cause	The ftp server fails to send message.
Alarm Prototype Description	Alarm occurred 00:07:21 01/01/2001 UTC alarm 16922 occurred %OAM% Send message to protocol error by MCP
Recommended Operations	Check whether FTP server configuration is correct and whether the connection is well.

16923

Message No.	16923
Default Security Level	6
Alarm Type	"ProcessingErrorAlarm"
NM Level	4
Cause	After enabling DHCP, the switch will download configuration file through TFTP circularly. When retry time is 10, about 4~5 minutes, version is not downloaded
Influence	Inform user of failure of downloading and suggest downloading again.
Recommended Operations	Stop DHCP automatic download configuration file function.

Alarm Description Prototype	Auto download config file fail Example: 00:57:29 01/01/2001 UTC alarm 16923 occurred %OAM% Auto download config file fail sent by MCP
Alarm Description	DHCP auto download configuration file retry fails.
Supported Devices	39,59,69

16924

Message No.	16924
Default Security Level	3
Alarm Recovery	Available
Alarm Type	QOS Alarm
NM Level	3
Cause	The utilization ratio that process uses CPU resource reaches defined high threshold.
Influence	Response to operation may be slow.
Related Alarms	16925 16926
Recommended Operations	It is normal that CPU resource is consumed too much in a short time. Use the show task detail command to view the utilization ratio that process uses CPU resource.
Alarm Description Prototype	Task %s current CPU load is: %d.%02d%% exceeds the highest Threshold %d%% The first %s is process name type. The first %d and second %d are peak value of utilization ratio that process uses CPU resource. The third %d is high threshold that process uses CPU resource. Alarm Generated An alarm 16924 level 3 occurred at 00:52:07 01/01/2001 UTC sent by UPC(MPU) 1 %OAM% Task ACL current CPU load is: 60.0% exceeds the highest Threshold 55% Alarm Recovery An alarm 16924 level 3 cleared at 00:53:07 01/01/2001 UTC sent by UPC(MPU) 1 %OAM% Task ACL current CPU load is: 50.0% under the highest Threshold 55%
Alarm Description	The utilization ratio that process uses CPU resource reaches defined high threshold.
Supported Devices	69 89

16925

Message No.	16925
Default Security Level	4
Alarm Recovery	Available

Alarm Type	QOS Alarm
NM Level	4
Cause	The utilization ratio that process uses CPU resource reaches defined medium threshold.
Influence	Response to operation may be slow.
Related Alarms	16924 16926
Recommended Operations	It is normal that CPU resource is consumed too much in a short time. Use the show task detail command to view the utilization ratio that process uses CPU resource.
Alarm Description Prototype	Task %s current CPU load is: %d.%02d%% exceeds the intermediate Threshold %d%% The first %s is process name type. The first %d and second %d are peak value of utilization ratio that process uses CPU resource. The third %d is medium threshold that process uses CPU resource. Alarm Generated An alarm 16924 level 4 occurred at 00:54:07 01/01/2001 UTC sent by UPC(MPU) 1 %OAM% Task ACL current CPU load is: 40.0% exceeds the intermediate Threshold 35% Alarm Recovery An alarm 16924 level 4 cleared at 00:55:07 01/01/2001 UTC sent by UPC(MPU) 1 %OAM% Task ACL current CPU load is: 30.0% under the intermediate Threshold 35%
Alarm Description	The utilization ratio that process uses CPU resource reaches defined medium threshold.
Supported Devices	6989

16926

Message No.	16926
Alarm Recovery	Available
Default Security Level	5
Alarm Type	QOS Alarm
NM Level	4
Cause	The utilization ratio that process uses CPU resource reaches defined low threshold.
Influence	Response to operation may be slow.
Related Alarms	16924 16925
Recommended Operations	It is normal that CPU resource is consumed too much in a short time. Use the show task detail command to view the utilization ratio that process uses CPU resource.
Alarm Description Prototype	Task %s current CPU load is: %d.%02d%% exceeds the lowest Threshold %d%% The first %s is process name type. The first %d and second %d are peak value of utilization ratio that process uses CPU resource. The third %d is low threshold that process uses CPU resource.

Alarm Generated

An alarm 16924 level 5 occurred at 00:56:07 01/01/2001 UTC sent by UPC(MPU) 1 %OAM% Task ACL current CPU load is: 20.0% exceeds the lowest Threshold 15%

Alarm Recovery

An alarm 16924 level 5 cleared at 00:57:07 01/01/2001 UTC sent by UPC(MPU) 1 %OAM% Task ACL current CPU load is: 10.0% under the lowest Threshold 15%

Alarm Description The utilization ratio that process uses CPU resource reaches defined low threshold.

Supported Devices 6989

OSPF Alarm

17408

Message No. 17408

Default Severity Level 6

Cause The port status shifts.

Recommended Operations Check whether OSPF status shift is normal according to the displayed alarm message. If it is abnormal, please check whether the configuration is correct and the corresponding status is correct.

17409

Message No. 17409

Default Severity Level 6

Cause The virtual link port status shifts.

Recommended Operations Check whether OSPF status shifts is normal according to the displayed alarm message. If it is abnormal, please check whether the configuration is correct and the corresponding virtual link port status is correct.

17410

Message No. 17410

Default Severity Level 6

Cause The neighbor status shifts.

Recommended Operations Check whether the OSPF status shifts is normal according to the displayed alarm message. If it is abnormal, please check whether

the configuration is correct and the interface status connected with neighbor is correct.

17411

Message No. 17411

Default Severity Level 6

Cause The virtual neighbor status shifts.

Recommended Operations Check whether the OSPF status shifts isnormal according to the displayed alarm message. If it is abnormal, please check whether the configuration is correct and the virtual link interface status connected with neighbor is correct.

17412

Message No. 17412

Default Severity Level 6

Cause Port authentication fails.

Recommended Operations Check whetehr the set authentication password of adjacent equipment at the interface corresponding to home equipment is consistent with the configuration on home equipment.

17413

Message No. 17413

Default Severity Level 6

Cause Virtual port authentication fails.

Recommended Operations Check whether the set authentication password of adjacent equipment at the virtual interface corresponding to home equipment is consistent with the configuration on home equipment.

17414

Message No. 17414

Default Severity Level 6

Cause The port receives error packets.

Recommended Operations Check whether the physical interface connection is reliable.

17415

Message No. 17415

Default Severity Level	6
Cause	The virtual port receives error packets.
Recommended Operations	Check whether the physical connection of interfaces forming the virtual interface is reliable.

17416

Message No.	17416
Default Severity Level	6
Cause	The database size is beyond the threshold.
Recommended Operations	After saving configuration information, re-enable relative module or restart equipment if possible.

17417

Message No.	17417
Default Severity Level	6
Cause	The interface configuration is wrong.
Recommended Operations	Modify the interface configuration to be inconsistent with the opposite end interface.

17418

Message No.	17418
Default Severity Level	6
Cause	The virtual interface configuration is wrong.
Recommended Operations	Modify the virtual interface configuration inconsistent with the opposite end interface.

17419

Message No.	17419
Default Severity Level	7
Cause	Packets are retransmitted at the interface.
Recommended Operations	Please check whether the network status is normal and the network load is too heavy.

17420

Message No. 17420

Default Severity Level 7

Cause Packets are retransmitted at the virtual interface.

Recommended Operations Please check whether the network status is normal and the network load is too heavy.

17421

Message No. 17421

Default Severity Level 6

Cause Fail to transmit MD5 report.

Recommended Operations Check whether the MD5 keyword configured at the interface is correct and valid.

17422

Message No. 17422

Default Severity Level 6

Cause Fail to distribute the memory.

Recommended Operations Please copy and save the information, then contact ZTE maintenance staff.

17423

Message No. 17423

Default Severity Level 6

Cause Receiving error request packet results in link-disconnection.

Recommended Operations Please check whether the interface physical link is stable.

17424

Message No. 17424

Default Severity Level 6

Cause The error sequence No. in DD packets the interface received results in link-disconnection.

Recommended Operations	Please check whether the interface physical link is stable.

17425

Message No.	17425
Default Severity Level	6
Cause	The route id not contained in Hello packet the interface received results in link-disconnection.
Recommended Operations	Please check whether the interface physical link is stable.

17426

Message No.	17426
Default Severity Level	6
Cause	Receiving Hello packet results in link-disconnection.
Recommended Operations	Please check whether the interface physical link is stable or the configuration is correct.

17427

Message No.	17427
Default Severity Level	6
Cause	Management Down results in link-disconnection.
Recommended Operations	Please check whether the disable process operation is executed.

17428

Message No.	17428
Default Severity Level	6
Cause	Physical interface Down result in link-disconnection.
Recommended Operations	Please check whether the shutdown operation is executed under the interface.

17429

Message No.	17429
Default Severity Level	6
Cause	Interface state change results in link-disconnection.

Recommended Operations Please check whether the interface state is changed.

RIP Alarm

17664

Message No. 17664

Default Severity Level 6

Cause RIP module fails to apply for the memory distribution.

Recommended Operations Please check whether the system memory utilization reaches the top and the system configuration information reaches or exceeds the permitted limits; If it reaches the top, consider to upgrade the equipment. If the system memory utilization does not reach the top, please contact ZTE maintenance staff.

17666

Message No. 17666

Default Severity Level 6

Cause RIP module fails to create timer.

Recommended Operations If the problem appears during command configuration, it may attempt a few minutes later. Please record the fault phenomenon and contact ZTE maintenance staff in time.

17667

Message No. 17667

Default Severity Level 6

Cause RIP route table is full and unable to add more RIP routes and new neighbors.

Recommended Operations Please check whether the configuration related to RIP protocol is correct and proper and whether the system running state is normal.

17670

Message No. 17670

Default Severity Level 6

Cause The RIP neighbor is not on the same subnet or the neighbor address is a network broadcast address.

Recommended Operations	Please check whether the configuration related to RIP protocol is correct and proper.

17671

Message No.	17671
Default Severity Level	6
Cause	Simple authentication has no keyword, so no authentication for packages.
Recommended Operations	Please check whether the configuration related to RIP protocol is correct and proper.

17672

Message No.	17672
Default Severity Level	6
Cause	RIP ignores invalid packet (which means packet failing to authenticate, or with incorrect version number, and not supporting command).
Recommended Operations	Please check whether the configuration related to RIP protocol is correct and proper.

17673

Message No.	17673
Default Severity Level	6
Cause	The RIP neighbor is invalid.
Recommended Operations	Please check whether the configuration related to RIP protocol is correct and proper, the network link status is normal and the router corresponding to RIP neighbor is running normally.

17676

Message No.	17676
Default Severity Level	6
Cause	The RIP interface status turns to down.
Recommended Operations	Please check whehter the link status is normal and whether the system is running normally.

17677

Message No. 17677

Default Severity Level 6

Cause The RIP interface status turns to up.

Recommended Operations Informational message. No action is required.

BGP Alarm

17920

Message No. 17920

Default Severity Level 6

Cause Fail to create BGP example.

Recommended Operations If possible, please delete some operations consuming resources, then try again.

17921

Message No. 17921

Default Severity Level 6

Cause Fail to create the protocol timer.

Recommended Operations If the problem appeared during command configuration, it may attempt a few minutes later.

17922

Message No. 17922

Default Severity Level 6

Cause Fail to create the neighbor.

Recommended Operations Please check whether the configuration is correct and proper, the system operation is normal and system memory application is to system maximum value.

17923

Message No. 17923

Default Severity Level	6
Cause	Fail to create the neighbor timer.
Recommended Operations	If the problem appears during configuration, it may attempt a few minutes later.

17924

Message No.	17924
Default Severity Level	6
Cause	BGP fails to acquire TCB for passive interception.
Recommended Operations	The link setup information acquired from TCP is wrong. Please check whether TCP is running normally first.

17925

Message No.	17925
Default Severity Level	6
Cause	BGP fails to acquire TCB for active link setup.
Recommended Operations	The link setup information acquired from TCP is wrong. Please check if TCP is running normally first.

17927

Message No.	17927
Default Severity Level	6
Cause	Fail to start the TCB of BGP passive interception interface.
Recommended Operations	Fail to start TCP for link setup. Please check if TCP is running normally first.

17928

Message No.	17928
Default Severity Level	6
Cause	Fail to start the TCB of BGP active interception interface.
Recommended Operations	Fail to start TCP for link setup. Please check whether TCP is running normally first.

17932

Message No. 17932

Default Severity Level 6

Cause The interface is down and the neighbor link is broken.

Recommended Operations Check whether the physical interface connection is normal.

17934

Message No. 17934

Default Severity Level 6

Cause Errors occur in reading the receiving buffer.

Recommended Operations Delete useless TCP connections created by BGP in the means of disabling and enabling the peer-to-peer.

17936

Message No. 17936

Default Severity Level 6

Cause The neighbor HOLDTIME is overtime.

Recommended Operations Check whether the connection with the one on the opposite end equipment is normal.

17938

Message No. 17938

Default Severity Level 6

Cause The state machine is wrong.

Recommended Operations Check whether the connection with the butting equipment is normal, and the system operation is well.

17940

Message No. 17940

Default Severity Level 6

Cause Received report is unidentifiable.

Recommended Operations Check the version information of the opposite end BGP, and check whether the line connection is correct and proper.

17941

Message No. 17941

Default Severity Level 6

Cause The report header is wrong.

Recommended Operations Check the version information of the opposite end BGP, and check whether the line connection is correct and proper.

17942

Message No. 17942

Default Severity Level 6

Cause Incorrect OPEN report.

Recommended Operations Check whether both peer-to-peer configuration of the opposite end is correct, especially whether an authentication password is configured.

17943

Message No. 17943

Default Severity Level 6

Cause Incorrect UPDATE report

Recommended Operations Check whether the opposite end BGP configuration is correct. Incorrect BGP configuration brings to transmitting error packets.

17944

Message No. 17944

Default Severity Level 6

Cause The neighbor receives update but no resources.

Recommended Operations Please check whether the system operation is normal, and the system resource occupancy is in normal range. After copying this alarm message, system resource occupancy and system configuration, contact with ZTE maintenance staff please.

17945

Message No. 17945

Default Severity Level 6

Cause	The neighbor receives the update but NLRI exceeds the maximum prefix length.
Recommended Operations	Please check whether the BGP protocol module configuration is correct and proper.

17946

Message No.	17946
Default Severity Level	6
Cause	Invalid routes are received.
Recommended Operations	Check whether the route design of transmitting end is correct and proper; because it might be loopback route.

17947

Message No.	17947
Default Severity Level	6
Cause	The neighbor receives update report, of which MR_REACH_NLRI is the VPN-IPV4 address cluster; but the RD domain is not 0, and BGP will ignore the domain.
Recommended Operations	Please check whether the BGP protocol configuration is correct, and network operation is normal.

17949

Message No.	17949
Default Severity Level	6
Cause	Incorrect NOTIFICATION report
Recommended Operations	Check the TX end settings.

17950

Message No.	17950
Default Severity Level	7
Cause	Fail to transmit report.
Recommended Operations	Check whether the port is operating normally.

17951

Message No.	17951

Default Severity Level	6
Cause	Fail to transmit OPEN report.
Recommended Operations	Check whether the port is operating normally.

17952

Message No.	17952
Default Severity Level	6
Cause	Fail to transmit KEEPALIVE report.
Recommended Operations	Check whether the port is operating normally.

17953

Message No.	17953
Default Severity Level	6
Cause	Fail to transmit NOTIFICATION report.
Recommended Operations	Check whether the port is operating normally.

17954

Message No.	17954
Default Severity Level	7
Cause	Fail to transmit UPDATE reachable report.
Recommended Operations	None, and system will try again one second later.

17955

Message No.	17955
Default Severity Level	7
Cause	Fail to transmit UPDATE unreachable report.
Recommended Operations	None, and system will try again one second later.

17956

Message No.	17956
Default Severity Level	6
Cause	SPOOL tries to send other report when it is not idle.

Recommended Operations	Check whether the port is operating normally.

17957

Message No.	17957
Default Severity Level	6
Cause	Fail to create SPOOL.
Recommended Operations	Please check whether the system operation is normal, and the system resource occupancy is in normal range.

17958

Message No.	17958
Default Severity Level	6
Cause	Fail to distribute memory.
Recommended Operations	Check whether the route quantity is to maximum, and system memory application is to the maximum value.

17959

Message No.	17959
Default Severity Level	6
Cause	Fail to insert route.
Recommended Operations	Check whether the route quantity is to maximum, and system memory application is to the maximum value.

17960

Message No.	17960
Default Severity Level	6
Cause	Distribution protocol fails to use route memory.
Recommended Operations	Check whether the route quantity is to maximum, and system memory application is to the maximum value.

17961

Message No.	17961
Default Severity Level	6
Cause	The status shifts.

Recommended Operations Check whether the status shift is normal according to the description in alarm messages. If it is abnormal, please check whether the system is running normally, the configuration is correct, the port and the opposite end are running normally.

17962

Message No. 17962

Default Severity Level 6

Cause Fail to obtain index number when establishing neighbors.

Recommended Operations Please check whether the BGP configuration is correct.

17963

Message No. 17963

Default Severity Level 6

Cause The neighbor fails to delete from GROUP.

Recommended Operations Please try to delete again.

17964

Message No. 17964

Default Severity Level 7

Cause Fails to transmit refresh packet.

Recommended Operations Please check whether the physical link is normal.

DRP Alarm

Syntax

18176

Message No. 18176

Default Severity Level 6

Cause Fail to create IPI example.

Recommended Operations If possible, perform state machine change again.

18177

Message No. 18177

Default Severity Level	6
Cause	Fail to create BGP example.
Recommended Operation	If possible, perform state machine change again or set the relevant parameters again.

18180

Message No.	18180
Default Severity Level	6
Cause	Fail to enable IPI example.
Recommended Operation	If possible, perform state machine change again.

18181

Message No.	18181
Default Severity Level	6
Cause	During AS No. setting, fail to enable IPI example again.
Recommended Operation	If possible, perform state machine change again or set the relevant parameters again.

18182

Message No.	18182
Default Severity Level	6
Cause	Fail to enable IPI example with a timer.
Recommended Operation	If possible, perform state machine change again or set the relevant parameters again.

18183

Message No.	18183
Default Severity Level	6
Cause	The IPI example fails (exact information is in the generated alarm message description, which differs as the configuration varies) to create OSPF example for ROUTE-ID.
Recommended Operation	If possible, perform state machine change again or set the relevant parameters again.

18184

Message No. 18184

Default Severity Level 6

Cause OSPF is not started, but it receives report.

Recommended Operation Check whether the relevant router configuration is correct.

18185

Message No. 18185

Default Severity Level 6

Cause No IFB matches the received OSPF report.

Recommended Operation Check whether the relevant router configuration is correct.

18186

Message No. 18186

Default Severity Level 6

Cause IFB DOWN, OSPF report discarded

Recommended Operation Check whether the relevant router configuration is correct and the interface status is normal.

18189

Message No. 18189

Default Severity Level 6

Cause Errors occur in IP synchronization route table.

Recommended Operation Check whether the router and interface is running well and the configuration is correct.

18190

Message No. 18190

Default Severity Level 6

Cause Fail to distribute memory.

Recommended Operation Check whehter the router running is normal, the configuration is proper and the system memory application is to maximum system operation limits.

18191

Message No. 18191

Default Severity Level 6

Cause Fail to insert route.

Recommended Operation Check whether the routing table exceeds the maximum quantity of running route items and whether the parameter configuration related to route is proper.

18192

Message No. 18192

Default Severity Level 6

Cause Fail to distribute route memory.

Recommended Operation Check whether the route parameter configuration is correct and proper.

18193

Message No. 18193

Default Severity Level 6

Cause Delete nonexistent routes.

Recommended Operation Check whether the router running is normal and all parameter configurations are correct.

18195

Message No. 18195

Default Severity Level 6

Alarm Recovery Unavailable

Alarm Type QoSAlarm

NM Level 5

Cause The VPN Route Limit function is set, not the warning-only. For example, in vrf configure mode, configure maximum routes 4 75. When a new routing is added to vrf, the current route items reaches the upper limit of the maximum(the first parametert, such as 4), then the alarm occurs.

Influence The new routing can not be added.

Related Alarms The alarm 18196 may occur before this alarm.

Recommended Operations Increase the routing maximum threshold according to the circumstance. Reduce the alarm. Configure Vpn route limit fuction, for

	example, maximum routes 100 75 to increase the routing maximum threshold(the first parameter).
Alarm Prototype Description	The routes limit of %s is exceeded %s is the vpn name that generates the alarm. An alarm 18195 level 6 occurred at 00:01:37 01/01/2001 UTC sent by MCP %DRP% The routes limit of VPN1 is exceeded
Alarm Description	The entering vrf routing exceeds the configured maximum threshold.
Supported Devices	T128, 69
Appendix Specification	N.A.

18196

Message No.	18196
Default Severity Level	6
Alarm Recovery	Unavailable
Alarm Type	QoSAlarm
NM Level	5
Cause	The VPN Route Limit function is set. For example, in vrf configure mode, configure maximum routes 4 75 or maximum routes 4 warning-only. When a new routing is added to vrf, the current route items(including the new routing) reaches the upper limit of the maximum(when configuring maximum routes 4 75, the alarm threshold is 4 * 75% =3, when configuring maximum routes 4 warning-only, the alarm threshold is 4 *100% =4), then the alarm occurs.
Related Alarms	18195
Recommended Operations	Increase the routing maximum threshold according to the circumstance. Reduce the alarm. Configure Vpn route limit fuction, manner one: magnify the alarm threshold(the second parameter). For example, use maximum routes 100 95 instead of maximum routes 100 75. Manner two: magnify the maximum threshold(the first parameter). For example, use maximum routes 40 warning-only instead of maximum routes 4 warning-only.
Alarm Prototype Description	The routes warning limit of %s is exceeded %s is the vpn name that generates the alarm. An alarm 18196 level 6 occurred at 00:01:02 01/01/2001 UTC sent by MCP %DRP% The routes warning limit of VPN1 is exceeded.
Alarm Description	The input vrf routing exceeds the configured alarm threshold.
Supported Devices	T128, 69

Appendix Specification N.A.

TCP Alarm

18433

Message No. 18433

Default Severity Level 6

Cause TCP waiting timeout duration does not end.

Recommended Operations Please wait patiently.

18434

Message No. 18434

Default Severity Level 6

Cause TCP starts TCB block incorrectly.

Recommended Operations Restart TCP.

18435

Message No. 18435

Default Severity Level 6

Cause TCP starts too many connections.

Recommended Operations Close or clear some TCP connections.

18436

Message No. 18436

Default Severity Level 6

Cause TCP sends the message of who am I.

Recommended Operations Please check whether the local TCP address is set.

18437

Message No. 18437

Default Severity Level 6

Cause	The port that TCP is to start is under application.
Recommended Operations	Clear existent TCP connection, and then try again.

18438

Message No.	18438
Default Severity Level	7
Cause	The IP version of packet received by TCP is incorrect.
Recommended Operations	Check whether the link status and network connection is normal.

18439

Message No.	18439
Default Severity Level	7
Cause	The checksum of packet received by TCP is wrong.
Recommended Operations	Check whether the network connection and operation is normal.

18440

Message No.	18440
Default Severity Level	6
Cause	The silent time received by TCP does not end.
Recommended Operations	Check whether the network connection and operation are normal.

18450

Message No.	18450
Default Severity Level	5
Cause	TCP receives packets with BGP MD5 authentication failure.
Recommended Operations	Check whether MD5 authentication setting is correct.

18451

Message No.	18451
Default Severity Level	4
Cause	TCP receives packets with wrong header length.

Recommended Operations	Check whether the network status and TCP connection are normal.

18452

Message No.	18452
Default Severity Level	4
Cause	TCP receives the packets with offset error.
Recommended Operations	Check whether the network status and TCP connection are normal.

18453

Message No.	18453
Default Severity Level	4
Cause	TCP receives the packets with tty security check failure.
Recommended Operations	Check whether the TCP connection reaches the maximum setting value.

18455

Message No.	18455
Default Severity Level	4
Cause	TCP sends allocate packets incorrectly.
Recommended Operations	Check whether the network operation and TCP connection are normal.

18456

Message No.	18456
Default Severity Level	7
Cause	TCP sends the packets with incorrect IP versions.
Recommended Operations	Check whether the remote IP address and TCP connection are normal.

18457

Message No.	18457
Default Severity Level	6
Cause	TCP fails in closing nonexistent connections.

Recommended Operations	Check whether the TCP connection is normal.

18458

Message No.	18458
Default Severity Level	3
Cause	TCP fails in closing connections in error status.
Recommended Operations	Check whether the TCP connection is normal.

18459

Message No.	18459
Default Severity Level	4
Cause	TCP retransmits allocate packets incorrectly.
Recommended Operations	Check whether the TCP connection and network status are normal.

18460

Message No.	18460
Default Severity Level	3
Cause	TCP fails in clearing nonexistent connections.
Recommended Operations	Check whether the TCP connection is normal.

18461

Message No.	18461
Default Severity Level	4
Cause	TCP calculates the available windows incorrectly.
Recommended Operations	Check whether the TCP connection is normal.

18463

Message No.	18463
Default Severity Level	4
Cause	When received BGP message, MD5 authentication fails.

Recommended Operations Check Whether the passwords in two ends of BGP are the same.

18464

Message No. 18464

Default Severity Level 4

Cause: PROTOCOL fails to send message to application procedure.

Recommended Operations Check Whether the passwords in two ends of BGP are the same.

UDP Alarm

18560

Message No. 18560

Default Severity Level 4

Cause UDP MP Initialization creates synchronous timer incorrectly.

Recommended Operations Restart UDP.

18561

Message No. 18561

Default Severity Level 3

Cause UDP module fails to apply for memory.

Recommended Operations Check whether the system is running normally. If necessary, save the configuration and then restart the router.

18562

Message No. 18562

Default Severity Level 7

Cause UDP receives the packets with wrong headers.

Recommended Operations Check whether the network connection and router running is normal.

18563

Message No. 18563

Default Severity Level	7
Cause	UDP receives the packets with wrong IP versions.
Recommended Operations	Check whether the network connection is normal and the system configuration is correct.

18564

Message No.	18564
Default Severity Level	7
Cause	UDP receives the packets with wrong checksum.
Recommended Operations	Check whether the network connection is normal.

IP Alarm

18689

Message No.	18689
Default Severity Level	2
Cause	RP fails to initialize routing table.
Recommended Operations	If possible, save the configuration and then restart the router. Please contact ZTE maintenance staff after saving this message.

18691

Message No.	18691
Default Severity Level	4
Cause	Fail to initialize the packet buffer.
Recommended Operations	Check whether the router running is normal.

18692

Message No.	18692
Default Severity Level	2
Cause	Fail to initialize the interface connection.

Recommended Operations If possible, restart the line board where the interface is located.

18720

Message No. 18720

Default Severity Level 6

Cause The interface is up.

Recommended Operations Informational message. No action is reqiured.

18721

Message No. 18721

Default Severity Level 6

Cause The interface is down.

Recommended Operations Check whether the interface cable is well and the system running is normal.

18722

Message No. 18722

Default Severity Level 4

Cause When establishing the interface, the programe fails to establish database nodes, which brings to mistakes on interface info.

Recommended Operations Look over the database nodes and confirm whether they run out of use. Please stop establishing interfaces if database nodes are used up.

18737

Message No. 18737

Default Severity Level 6

Cause Receive the packet of undefined type.

Recommended Operations Check whether the network running is well and the system configuration is proper.

18738

Message No. 18738

Default Severity Level 6

Cause	The IP header length of received packets is too short.
Recommended Operations	Check whether the network running is well.

18739

Message No.	18739
Default Severity Level	6
Cause	The length of received IP packets is wrong.
Recommended Operations	Check whether the network connection and operation are in sound conditions.

18740

Message No.	18740
Default Severity Level	7
Cause	The received IP packet version is wrong.
Recommended Operations	Check whether the network connection and operation are in sound conditions.

18741

Message No.	18741
Default Severity Level	7
Cause	The received IP packet checksum is wrong.
Recommended Operations	Check whether the network connection and operation are in sound conditions, and whether the system configuration are correct.

18742

Message No.	18742
Default Severity Level	7
Cause	Receiving IP packets with illegal source address.
Recommended Operations	Check whether the network connection and operation are normal, and whether anybody is attacking the network.

18743

Message No.	18743
Default Severity Level	6

Cause	Receiving IP packets with illegal destination address.
Recommended Operations	Check whether the network connection and operation are normal, and whether anybody is attacking the network.

18744

Message No.	18744
Default Severity Level	9
Cause	The destination address of received IP packet is unreachable.
Recommended Operations	Check whether the system configuration is correct.

18745

Message No.	18745
Default Severity Level	7
Cause	The protocol type of received IP packet is unidentifiable.
Recommended Operations	Check whether the system configuration is correct.

18752

Message No.	18752
Default Severity Level	5
Cause	Fail in IP splicing operation.
Recommended Operations	If a large amount of such alarms occur continuously, please check whether the system running is normal.

18754

Message No.	18754
Default Severity Level	5
Cause	IP packets regrouping is overtime.
Recommended Operations	Check whether the network running status is normal.

18784

Message No.	18784
Default Severity Level	4
Cause	route-map is configured on xx (digital No.) line card and there is no way to be valid.

Recommended Operations	Please check whether the enabled route-map configuration on the line card is reaching to system permitted limit configuration; if no, contact ZTE maintenance staff in time after recording the information.

18785

Message No.	18785
Default Severity Level	4
Cause	route-map configuration has no way to be valid.
Recommended Operations	Please check whether the enabled route-map configuration is reaching to system permitted limit configuration; if not, contact ZTE maintenance staff in time after recording the information.

18786

Message No.	18786
Default Severity Level	4
Cause	Policy route has been configured with too many sequence item, which exceeds the system memory scope.
Recommended Operations	Please delete the unavailable policy route and reconfigure it.

18787

Message No.	18787
Default Severity Level	4
Cause	Too many ACL is applied in one line card.
Recommended Operations	No ACL can be applied in this line card unless to release one ACL.

18790

Message No.	18790
Default Severity Level	4
Cause	Too many ACL regulation is applied in one line card.
Recommended Operations	Delete some ACL regulation in this line card or delete some ACL on this line card.

18791

Message No.	18791

Default Severity Level	5
Cause	Too many ACL regulation is applied in one line card.
Recommended Operations	If alarm disappears after a while, then it means that instant memory occupancy is too much. It makes no influence. If alarm sustains, check whether memory occupancy reaches the maximum and the configuration information reaches or exceeds the threshold. If the memory occupancy reaches the threshold, please upgrade the device. Or contact with ZTE corporation.

18794

Message No.	18794
Default Severity Level	4
Cause	ACL module of NPC fails to dispose message.
Recommended Operations	This alarm is a prompt. It is usually caused by instant busyness of interior communication. This alarm disappears later. If the alarm continues, please contact with ZTE Corporation.

18832

Message No.	18832
Default Severity Level	6
Alarm Recovery	Unavailable
Alarm Type	ProcessingErrorAlarm
NM Level	5
Cause	When LSP pings TE tunnel, the setting to option Size is so large that the size of LSP ping packet is larger than MTU of outgoing interface, where packet segmentation is needed. But packet cannot be segmented when LSP pings TE tunnel.
Influence	Fails to send LspPing packet and prints "Q". LspPing can not get through.
Recommended Operations	Reduce the setting to option Size in LSP PING TE tunnel.
Alarm Prototype Description	Alarm occured 02:09:51 11/09/2098 UTC alarm 18832 occurred %IP% Operation failed while fragmentize RSVP datagram sent by UPC(RPU) 1
Alarm Description	Because the set option size is too big, the LspPing packet is larger than the MTU of the outgoing interface. RSVP packet cannot be segmented when LSP pings TE tunnel.
Supported Devices	T128, T1200

18833

Message No.	18833
Default Severity Level	4
Alarm Recovery	Unavailable
Alarm Type	ProcessingErrorAlarm
NM Level	5
Cause	Invalid ippool.
Influence	Users can not get online.
Recommended Operations	Through turnning on the IPPOOL debug switch, check the origin of the invalid disposal(from the DHCPPOOL or PPP module).
Alarm Prototype Description	Failed to process ippool [%s] %s: the set ip pool nameippool does not exist Alarm occurred 0:29:52 08/13/2008 UTC alarm 18833 occurred %IP% failed to process ippool [invalidPool]
Alarm Description	Invalid ippool
Supported Devices	All.

18834

Message No.	18834
Default Severity Level	4
Alarm Recovery	Unavailable
Alarm Type	ProcessingErrorAlarm
NM Level	5
Cause	Ippool address block number reaches the threshold.
Influence	Users can not get online.
Recommended Operations	Turn on the IPPOOL debug to obtain more detailed information. Ippool address block number reaches the threshold. Force some user down-line in the relative service module(DHCP or PPP) and let the newer access.
Alarm Prototype Description	ippool bitmap has reached max number 4096 4096 is the upper threshold of IPPOOL. Alarm occurred 20:33:24 08/13/2008 UTC alarm 18834 occurred %IP% ippool bitmap has reached max number 4096 sent by UPC(RPU) 2
Alarm Description	Ippool address block number reaches the threshold.

Supported Devices All.

18835

Message No. 18835

Default Severity Level 4

Alarm Recovery Unavailable

Alarm Type QoSAlarm

NM Level 3

Cause The current ingress/egress traffic utilization exceeds the set threshold(80% by default).

Recommended Operations Increase the threshold.

Set the flow-threshold-input to 100.

```
zxr10(config)#int fei_1/1
zxr10(config-if)#flow-threshold-input 100
```

Set flow-threshold-output to 100.

```
zxr10(config-if)#flow-threshold-output 100
```

Alarm Prototype Description current output traffic is %d, over the threshold is %d

current input traffic is %d, over the threshold is %d

The first %d: current traffic utilization

The second %d: the set traffic utilization

06:18:43 06/19/2002 UTC alarm 18335 occurred %IP% current output traffic is 90%,over the threshold is 85% on fei_8/1 sent by UPC(RPU) 1

06:18:43 06/19/2002 UTC alarm 18335 occurred %IP% current input traffic is 90%,over the threshold is 85% on fei_8/1 sent by UPC(RPU) 1

Alarm Description The current ingress/egress traffic utilization exceeds the set threshold.

Supported Devices T128, T1200

IGMP Alarm

18944

Message No. 18944

Default Severity Level 6

Cause A member joins IGMP multicast group.

Recommended Operations	N.A.

18945

Message No.	18945
Default Severity Level	6
Cause	A member leaves IGMP multicast group.
Recommended Operations	Check whether related configurations of IGMP protocol are correct and proper and whether any messages about joining and leaving of IGMP group member are received.

ARP Alarm

19712

Message No.	19712
Default Severity Level	6
Cause	Dynamic ARP item MAC address is changed.
Recommended Operations	Please check whether the ARP item MAC address is legal; if it is illegally changed, bind correct MAC address manually to protect legal users from being attacked.

19713

Message No.	19713
Default Severity Level	6
Cause	It exceeds the item limitation (based on interface/overall) protected by ARP.
Recommended Operations	Check whether ARP protection is configured and whether anybody attacks balefully to pour ARP table fully.

19714

Message No.	19714
Default Severity Level	6
Cause	The received ARP report source MAC address is the same as local MAC address.

Recommended Operations Check whether the MAC address is legal.

19715

Message No. 19715

Default Severity Level 6

Cause The received ARP source IP address is conflict with local interface address.

Recommended Operations Check whether the IP address is legal and whether two sets of equipments have the same IP address.

19716

Message No. 19716

Default Severity Level 6

Cause Enable ARP inspection for DHCP Snooping function. If source address of the received ARP packet is an illegal DHCP user, then drop it.

Recommended Operations Please check whether ARP inspection is enabled for DHCP Snooping function.

19717

Message No. 19717

Default Severity Level 6

Cause IP POOL filtering function is enabled on SUPERVLAN interface. If the source address of received ARP packet is not in IP POOL segment, then drop it.

Recommended Operations Please check whether IP POOL filtering function is enabled on SUPERVLAN interface and check IP pool configuration information. If filtering is not needed here, please disable this function.

19720

Message No. 19720

Default Severity Level 5

Alarm Recovery Unvailable

Alarm Type Environmental Alarm

NM Level 3

Cause Specify that at most 100 ARP packets can be received on interface per second. If the received packets are more than 100, drop the

	superfluous packets and interface is believed under ARP attack. Meanwhile, alarm appears.
Influence	Operation response may be slow.
Recommended Operations	Reduce system load.
Alarm Prototype Description	Arp-Flood 03:16:51 01/18/2001 UTC alarm 19720 occurred %ARP% Arp-Flood on fei_1/1 sent by MCP
Alarm Description	Interface is under ARP attack and received ARP packets are more than 100.
Supported Devices	GAR18/28/38
Appendix Specification	The platform V2.8.01b and the upgrade versions support this alarm.

IS-IS Alarm

19968

Message No.	19968
Default Severity Level	6
Cause	Neighbors set up the adjacent relationship.
Recommended Operations	N.A.

19969

Message No.	19969
Default Severity Level	6
Cause	The neighbor is invalid.
Recommended Operations	Check whether the system operation and network connection is normal, and whether the configuration is correct.

19970

Message No.	19970
Default Severity Level	5
Cause	Receive LSP packet from an invalid neighbor.

Recommended Operations	Check whether the system configuration is correct.

19972

Message No.	19972
Default Severity Level	6
Cause	Receive LSP packet from an unknown neighbor.
Recommended Operations	Check whether the system configuration is correct.

19974

Message No.	19974
Default Severity Level	6
Cause	Neighbor fails in authentication.
Recommended Operations	Check whether the system configuration is correct and whether it is consistent with the configuration of the opposite end.

19975

Message No.	19975
Default Severity Level	6
Cause	LSP packet fails in authentication.
Recommended Operations	Check whether the system configuration is correct and whether it is consistent with the configuration of the opposite end.

19976

Message No.	19976
Default Severity Level	6
Cause	SNP packet fails in authentication.
Recommended Operations	Check whether the system configuration is correct and whether it is consistent with the configuration of the opposite end.

19977

Message No.	19977
Default Severity Level	6
Cause	Receive illegal packets.

Recommended Operations	Check whether the system configuration is correct.

19978

Message No.	19978
Default Severity Level	6
Cause	Fail to add IS-IS route.
Recommended Operations	Check whether the system running status is normal and the system configuration is proper.

19979

Message No.	19979
Default Severity Level	6
Cause	Fail in IS-IS memory allocation.
Recommended Operations	Check the system running status. If possible, save the system configuration information and then restart the system.

19980

Message No.	19980
Default Severity Level	6
Cause	When ISIS runs TE path calculation, if no LSP entry or multiple corresponding LSP entries are found according to one given router-id, this alarm will be generated.
Recommended Operations	Check the network configuration. Check whether the same TE router-id is configured on multiple routers or whether this TE router-id is configured on no router.

19981

Message No.	19981
Default Severity Level	6
Cause	When ISIS is in GR process, if system control module doesn't support this boot mode, this alarm will be generated.
Recommended Operations	Check whether the hot standby state of support module is correct.

19982

Message No.	19982

Default Severity Level	6
Cause	When configuring ISIS aggregation, if there is no additional space for ISIS LSP packet, the alarm will be generated.
Recommended Operations	Please set parameter range 32 in command System-ID.

19983

Message No.	19983
Default Severity Level	6
Alarm Recovery	unavailable
Alarm Type	EquipmentAlarm
NM Level	5
Cause	When configuring ISIS aggregation, if there is no additional space for ISIS LSP packet, the alarm will be generated. ISIS protocol regards the interface failure. The reason for interface invalid may be as follows: If this interface is deleted, ISIS protocol regards that this interface is invalid. If ISIS can not find the corresponding physical interface, then it regards that this interface is invalid. If the interface encapsulation type changes, ISIS regards that this interface is invalid instantly. If this interface switchovers from one ISIS instance to another, ISIS regards that this interface is invalid instantly. This interface is up physically, but ISIS does not regard it as UP. For example, if the interface IP address is deleted suddenly, ISIS regards that this interface is invalid.
Influence	Notice ISIS that this interface is invalid.
Alarm Prototype Description	Port %s (port num %d) change from UP to DOWN %s: interfacer name %d: interface number Port %s (port num %d) type change from %s to %s The first %s: interface name %d: interface number The second %s: The string "BROADCAST" or "P2P". The third %s: The string "P2P" or "BROADCAST". Port %s (port num %d) is deleted %s: interface name %d: interface number Port %s (port num %d) is not found, delete it %s: interface name

%d: interface number

Port %s (port num %d) remove from instance %d %s: interface number

The first %d: interface number

The second %d: ISIS instance number,from 1 to 10000

17:13:47 06/25/2008 UTC alarm 19983 occurred %ISIS% Port fei_1/1 (port num 18) change from UP to DOWN.

17:17:28 06/30/2008 UTC alarm 19983 occurred %ISIS% Port fei_1/1 (port num 18) remove from instance 2

Supported Device ZXR10 series router/switch.

RMON Alarm

20737

Message No. 20737

NM Level 6

Cause RMON is grouped incorrectly.

Recommended Operations Check whether the command input is correct.

20746

Message No. 20746

NM Level 6

Cause The message header received by RMON module is wrong.

Recommended Operations Check whether the system running status is normal and the command input is correct.

20747

Message No. 20747

NM Level 6

Cause The message data received by RMON module is wrong.

Recommended Operations Check whether the system running status is normal and the command input is correct.

20748

Message No. 20748

NM Level 6

Cause The message return area received by RMON module is wrong.

Recommended Operations Check whether the system running status is normal.

20757

Message No. 20757

NM Level 6

Cause The command ID received by RMON module is wrong.

Recommended Operations Check whether the command configuration is correct and the system running is normal.

20758

Message No. 20758

NM Level 6

Cause The command parameter received by RMON module is wrong.

Recommended Operations Check whether the command configuration parameter is correct.

20759

Message No. 20759

NM Level 6

Cause The command parameter quantity received by RMON module is wrong.

Recommended Operations Check whether the command configuration parameter is correct.

20776

Message No. 20776

NM Level 6

Cause The RMON timer is wrong.

Recommended Operations Check whether the system running status is normal, and being able to perform the relevant RMON configurations again.

20793

Message No. 20793

NM Level 6

Cause The resources do not exist.

Recommended Operations Check whether RMON configuration command is correct and the relevant system parts are normally running.

URPF Alarm

21248

Message No. 21248

NM Level 5

Cause Source route check failure alarms.

Recommended Operations N.A.

ACL Alarm

21762

Message No. 21762

NM Level 5

Cause There is wrong drive when binding ACL to the interface. The reason is that much QoS is applied in ACL.

Recommended Operations Reduce QoS application in ACL and bind again.

21764

Message No. 21764

NM Level 5

Cause There is wrong drive when binding ACL to the interface.

Recommended Operations Check ACL QoS configuration and reduce QoS quantity and ACL rule number. Try again.

21773

Message No. 21773

NM Level 6

Cause When Line-card reboots, one type of ACL: ACL+name(for example ACL test) is deleted.

Recommended Operations N.A.

Alarm Prototype Description Alarm occurred

05:46:35 04/16/2003 UTC alarm 21773 occurred %IP% SYNC ACLs, NPC send message failedsent by MEC 1

21774

Message No.	21774
Alarm Type	ProcessingErrorAlarm
NM Level	5
Cause	Because one securityaccess item is set to ON state. Multiple security access entries are in ON state on a non-stack master device.
Influence	The item in ON state currently will not take effect when the alarm occurs.
Recommended Operations	Reduce the number of entries whose state are ON, for which we can set the states of entries not needed to OFF and re-set the state of specific entry to ON.
Alarm Prototype Description	"Too many security access entities are enabled" For example: An alarm 21774 level 5 occurred at 00:08:59 01/01/2001 UTC sent by Stack Slave DevId 2 %ACL% Too many security access entities are enabled
Alarm Description	Multiple security access entries are in ON state on a non-stack master device.
Supported Devices	ZXR10 59/52 series.

21775

Message No.	21775
Alarm Type	ProcessingErrorAlarm
NM Level	5
Cause	Error occurs when doing Securityaccess operation. It's a prompt used when operation error occurs on a non-stack master device in stack system.
Influence	The current operation is invalid.
Recommended Operations	Retry; delete partial entries whose states are ON or set them to OFF and retry
Alarm Prototype Description	"Security access bind ip and mac error at driver" Alarm occured: An alarm 21775 level 5 occurred at 00:08:59 01/01/2001 UTC sent by Stack Slave DevId 2 %ACL% Security access bind ip and mac error at driver.
Alarm Description	The drive operation is error on a non-stack master device.
Supported Devices	ZXR10 59/52 series.

21776

Message No.	21776
Default Severity Level	5

Alarm Type	ProcessingErrorAlarm
NM Level	5
Cause	When adding a security access entry, we find that the same entry has existed. Generally, this alarm will not occur. It's a prompt used when operation error occurs on a non-stack master device in stack system.
Recommended Operations	Retry with another security access entry name; if this problem still exists, it's an internal processing consistency problem and please contact ZTE engineer.
Alarm Prototype Description	"The same security access entity already exists" Alarm occurred An alarm 21776 level 5 occurred at 00:08:59 01/01/2001 UTC sent by Stack Slave DevId 2 %ACL% A same security access entity already exists.
Alarm Description	When adding a security access entry, we find that the same entry has existed.
Supported Devices	ZXR10 59/52 series.

21777

Message No.	21777
Default Severity Level	5
Alarm Type	ProcessingErrorAlarm
NM Level	5
Cause	It is abnormal when operating on security access entries and this alarm will not occur generally. It's a prompt used when operation error occurs on a non-stack master device in stack system.
Influence	The current operation will not take effect.
Recommended Operations	It's an internal processing error. Please contact ZTE engineer.
Alarm Prototype Description	"Some error occurred" Alarm occurred Example: An alarm 21777 level 5 occurred at 00:08:59 01/01/2001 UTC sent by Stack Slave DevId 2 %ACL% Some error occurred.
Alarm Description	It is abnormal operating on security access entries on a non-stack master device in stack system.
Supported Devices	ZXR10 59/52 series.

VRRP Alarm

22016

Message No. 22016

Default Severity Level 6

Cause vrrp status switchover notice

Recommended Operations: Please check whether the status switchover is normal. If not, copy the alarm information and contact ZTE maintenance staff.

MAC Alarm

22784

Message No. 22784

NM Level 6

Cause MAC address reaches to the MAC quantity limitation set at port.

Recommended Operations Please check the port MAC address quantity settings. If it alarms with 22785 alternately, then, check if loop exists.

22785

Message No. 22785

NM Level 6

Cause After MAC address reaches to the MAC quantity limitation set at port, it is lower than the set quantity limitation.

Recommended Operations Please check port MAC address quantity setting and check if anybody attacks balefully; if it alarms with 22784 alternately, then, check if loop exists, and if anybody attacks balefully.

22786

Message No. 22786

NM Level 6

Cause Fail to write driver MAC address.

Recommended Operations If fail to write driver continuously, shut it down please and check if the hardware is connected well.

22787

Message No. 22787

NM Level 6

Cause Turn into protection status.

Recommended Operations Check whether the protection is configured and whether anybody attacks balefully.

22788

Message No. 22788

NM Level 6

Cause Exit the protection status.

Recommended Operations Check whether the protection is configured and whether anybody attacks balefully.

22789

Message No. 22789

NM Level 6

Cause MAC address shifts from one port to other port.

Recommended Operations Check whether loop exists. If not, then, check whether the same MAC address exists on different ports.

22790

Message No. 22790

NM Level 6

Cause State changes of spanning tree: if the specific instance under specific port changes from forwarding state to blocking state, dynamic MAC address of this port will be deleted.

Recommended Operations N.A.

22792

Message No. 22792

NM Level 6

Cause Outgoing interface of MAC address or inner outgoing tag changes.

Recommended Operations	Check whether there is any loop.

22793

Message No.	22793
Default Security Level	6
Alarm Recovery	None
Alarm Type	"EquipmentAlarm"
NM Level	5
Cause	The number of MAC addresses reaches the threshold set by VLAN.
Influence	This VLAN can't continue learning MAC address.
Related Alarms	22794
Recommended Operations	None
Alarm Description Prototype	"< VLAN %4d > MAC address number threshold reached" %s vlan id Example: 00:04:21 01/01/2001 UTC alarm 22793 occurred %MAC% < VLAN 1 > MAC address number threshold reached sent by MEC 1
Alarm Description	The number of MAC addresses reaches the threshold set by VLAN.
Supported Devices	59A 69 89

22794

Message No.	22794
Default Security Level	6
Alarm Recovery	None
Alarm Type	"EquipmentAlarm"
NM Level	5
Cause	When the number of MAC addresses reaches the threshold set by VLAN, because the number decreases the current number is lower than the number set by VLAN again.
Influence	This VLAN can continue learning MAC address.
Related Alarms	22793
Recommended Operations	None
Alarm Description Prototype	"< VLAN %4d > MAC address number drop to threshold" %s vlan id Example: 00:09:10 01/01/2001 UTC alarm 22794 occurred %MAC% < VLAN 1 > MAC address number drop to threshold sent by MEC 1

Alarm Description	The number of MAC addresses is lower than the threshold set by VLAN.
Supported Devices	59A6989

22795

Message No.	22795
Default Security Level	6
Alarm Recovery	None
Alarm Type	"EquipmentAlarm"
NM Level	5
Cause	The MAC event number reaches the maximum value.
Influence	The MAC event number reaches the maximum value, need apply for room.
Recommended Operations	None
Alarm Description Prototype	"MAC event number threshold reached"
Alarm Description	The MAC event number reaches the maximum value.
Supported Devices	None
Appendix Specification	This alarm is not supported by any of version at present.

22796

Message No.	22796
Default Security Level	6
Alarm Recovery	None
Alarm Type	"EquipmentAlarm"
NM Level	5
Cause	When the interface is bound with smartgroup, if physical interface configures permanent mac alarm need to promprt that permanent mac address should be deleted.
Influence	prompt permanent MAC deletion
Recommended Operations	None
Alarm Description Prototype	"< Port %s > Permanent MAC address canceled"
Alarm Description	When the interface is bound with smartgroup, if physical interface configures permanent mac alarm need to promprt that permanent mac address should be deleted.
Supported Devices	None

Appendix Specification	This alarm is not supported by any of version at present.

22797

Message No.	22797
Default Security Level	6
Alarm Type	"EquipmentAlarm"
NM Level	5
Cause	MAC learning mode is set as micode-learning and the current higig is opened by learning.
Influence	The learning mode can't be configured micode-learning.
Recommended Operations	set learning mode as mac learn special.
Alarm Description Prototype	"<MAC Table>mode in micode-learning,please input:mac learn special" Example 00:43:57 01/01/2001 UTC alarm 22797 occurred %MAC% <MAC Table>mode in micode-learning, please input:mac learn special sent by MEC 1
Alarm Description	The learning mode is micode-learning and need to be switched to learn special.
Supported Devices	6989.

22798

Message No.	22798
Default Security Level	6
Alarm Type	"EquipmentAlarm"
NM Level	5
Cause	Permanent MAC address number reaches the upper limit.
Influence	can’t continue configuring permanent MAC address
Alarm Description Prototype	"Permanent MAC address number threshold reached" %d service number Example: 00:25:00 01/01/2001 UTC alarm 22798 occurred %MAC% Permanent MAC address number threshold reached
Alarm Description	Permanent MAC address number reaches the upper limit.
Supported Devices	59A,69,89

Loop Detect

23296

Message No. 23296

Default Security Level 4

Alarm Type "EquipmentAlarm"

NM Level 5

Cause Find the interface has a loop.

Influence
1. Find interface has a loop in a vlan.
2. Find interface has a loop.

Alarm Description Prototype
1. Find interface loop in vlan %u

   %u vlan Id
2. Find interface loop

Example:

10:08:19 10/29/2008 UTC alarm 23296 occurred % LOOPDETECT % Find interface loop in vlan 200 sent by NPC 1

Alarm Description Interface has a loop.

Supported Devices 69,89

DHCP Alarm

23808

Message No. 23808

NM Level 5

Cause DHCP user obtains IP address and gets online. DHCP user releases IP address and gets offline.

Recommended Operations N.A.

23809

Message No. 23809

Default Severity Level 5

Alarm Recovery Available

Alarm Type CommunicationAlarm

NM Level 5

Cause	The IP address obtained from DHCP CLIENT is already used in the network.
Influence	IP address that the interface obtained is invalid.
Recommended Operations	Check DHCP configuration on the device.
Alarm Prototype Description	IP address %s has been used %s: obtained IP address Alarm occured: 15:52:13 01/22/2008 UTC alarm 23809 occurred %DHCP% IP address 1.1.1.1 has been used sent by UPC 1
Alarm Description	The IP address obtained from DHCP CLIENT is already used in the network.
Supported Devices	ZXR10 5900.

23810

Message No.	23810
Default Severity Level	5
Alarm Recovery	Unavailable
Alarm Type	CommunicationAlarm
NM Level	5
Cause	The user configure the IP address by manual which brings to that the IP address applied by DHCP CLIENT can not be withdrawed by DHCP SERVER immediately.
Recommended Operations	Disable DHCP CLIENT module under the interface, then configure the interface IP address by manual.
Alarm Prototype Description	operation will result in lease ip cann't reclaim by DHCP server immediately. Alarm occured: 15:00:13 01/22/2008 UTC alarm 23810 occurred %DHCP% operation will result in lease ip cann't reclaim by DHCP server immediately sent by MCP. Alarm Prototype Description:
Alarm Description	The user configure the IP address by manual which brings to that the IP address applied by DHCP CLIENT can not be withdrawed by DHCP SERVER immediately.
Supported Devices	ZXR10 5900.

23811

Message No.	23811
Default Severity Level	6
Alarm Recovery	Unavailable
Alarm Type	ProcessingErrorAlarm

NM Level	5
Cause	The across network section roaming switch appears in DHCP Relay or DHCP server user. But the roaming switch is off.
Influence	Users with roaming switch can not obtain IP address.
Recommended Operations	Turn on the roaming switch to let user launch DHCP request again. Use the following command: routerA(config)#ip dhcp ramble
Alarm Prototype Description	"verifying -illegal user %s from %s !" The first s: user mac address! The second s: L3 interface name of user access! Alarm occured: 16:28:43 07/15/2008 UTC alarm 23811 occurred % DHCP % verifying -illegal user 00 C0.0000 .0001 from vlan100! sent by NPC 2
Alarm Description	The across network section roaming switch appears in DHCP Relay or DHCP server user. But the roaming switch is off.
Supported Devices	ZXR10 3900, 5900, 6900 series switch. T64E, T128, T600, T1200 series router.

23812

Message No.	23812
Default Severity Level	6
Alarm Recovery	Unavailable
Alarm Type	ProcessingErrorAlarm
NM Level	5
Cause	DHCP Relay agent address is not configured in the L3 interface that the DHCP users access.
Influence	The user in L3 interface can not obtain the IP address.
Recommended Operations	Configure DHCP Relay agent address in the L3 interface to let user launch DHCP request again. Use the following command: routerA(config-if)#ip dhcp relay agent 200.1.1.1
Alarm Prototype Description	relay have no valid agent configure! Alarm occured: 16:53:11 07/15/2008 UTC alarm 23812 occurred % DHCP % relay have no valid agent configure sent by NPC 2
Alarm Description	DHCP Relay agent address is not configured in the L3 interface that the DHCP users access.
Supported Devices	ZXR10 3900, 5900, 6900 series switch. T64E, T128, T600, T1200 series router.

23813

Message No.	23813
Default Severity Level	6
Alarm Recovery	Unavailable
Alarm Type	ProcessingErrorAlarm
NM Level	5
Cause	DHCP Relay agent address is not the local interface address in the L3 interface that the DHCP users access.
Influence	The user in L3 interface can not obtain the IP address.
Recommended Operations	Check whether the DHCP Relay agent address and the DHCP Relay layer-3 interface address is matching.
Alarm Prototype Description	relay agent %s is not %s add! The first %s DHCP Relay agent address The second %s L3 interface name of user access interface Alarm occured: 14:03:33 07/16/2008 UTC alarm 23813 occurred % DHCP % relay agent 100.1.1.1 is n ot vlan100 addr sent by NPC
Alarm Description	DHCP Relay agent address is not the local interface address in the L3 interface that the DHCP users access.
Supported Devices	ZXR10 3900, 5900, 6900 series switch. T64E, T128, T600, T1200 series router.

23814

Message No.	23814
Default Severity Level	6
Alarm Recovery	Unavailable
Alarm Type	ProcessingErrorAlarm
NM Level	5
Cause	The set DHCPRelayserver is invalid.
Influence	The user in L3 interface can not obtain the IP address.
Recommended Operations	Check whether the DHCP Relay Server address is configured in DHCP Relay layer-3 interface.
Alarm Prototype Description	relay have no valid server configure! Alarm occurred 14:23:17 07/16/2008 UTC alarm 23814 occurred %MLD% relay have no valid server configure sent by NPC 2
Alarm Description	DHCP Relay Server address is not configured in the L3 interface that the DHCP users access
Supported Devices	ZXR10 3900, 5900, 6900 series switch.

T64E, T128, T600, T1200 series router.

23815

Message No.	23815
Default Severity Level	6
Alarm Recovery	Unavailable
Alarm Type	ProcessingErrorAlarm
NM Level	5
Cause	DHCP Relay Server address is the local VRRP address in the L3 interface that the DHCP users access.
Recommended Operations	Check whether the DHCP Relay Server address is the local VRRP address in DHCP Relay layer-3 interface. If it is the local VRRP address, then configure the DHCP Relay server again.
Alarm Prototype Description	relay server %s is local vrrp addr s IP address of DHCP Relay Server Alarm occurred 11:17:08 07/17/2008 UTC alarm 23815 occurred % DHCP % relay server 100.1.1.3 is local vrrp addr sent by NPC2
Alarm Description	DHCP Relay Server address is the local VRRP address in the L3 interface that the DHCP users access.
Supported Devices	ZXR10 3900, 5900, 6900 series switch. T64E, T128, T600, T1200 series router.

23816

Message No.	23816
Default Severity Level	6
Alarm Recovery	Unavailable
Alarm Type	ProcessingErrorAlarm
NM Level	5
Cause	DHCP Relay Server address is the local address in the L3 interface that the DHCP users access.
Influence	The user in L3 interface can not obtain the IP address.
Recommended Operations	Check whether the DHCP Relay Server address is the local address in DHCP Relay layer-3 interface. If it is the local address, then configure the DHCP Relay server again.
Alarm Prototype Description	relay server %s is local vrrp addr sIP address of DHCP Relay Server Alarm occurred 13:21:28 07/17/2008 UTC alarm 23816 occurred % DHCP % relay server 100.1.1.1 is local IP addr sent by NPC 2

Alarm Description	DHCP Relay Server address is the local address in the L3 interface that the DHCP users access.
Supported Devices	ZXR10 3900, 5900, 6900 series switch. T64E, T128, T600, T1200 series router.

23817

Message No.	23817
Default Severity Level	6
Alarm Recovery	Unavailable
Alarm Type	ProcessingErrorAlarm
NM Level	5
Cause	DHCP Relay Server address is the local address in the L3 interface that the DHCP users access.
Recommended Operations	Check whether the DHCP destination is reachable and whether the configuration is correct.
Alarm Prototype Description	ailed to send %s from %s to %s (%s) The first s Packet type of DHCP; The second s source ip address; The third s dest ip address; The fourth s the reason of failure ; Alarm occurred 17:24:09 07/17/2008 UTC alarm 23817 occurred % DHCP % failed to seng DHCPDISCOVER from 100.1.1.1 to 100.1.2.1(no route) sent by NPC 2
Alarm Description	Fails to send DHCP packet.
Supported Devices	ZXR10 3900, 5900, 6900 series switch. T64E, T128, T600, T1200 series router.

23818

Message No.	23818
Default Severity Level	6
Alarm Recovery	Unavailable
Alarm Type	ProcessingErrorAlarm
NM Level	5
Cause	The routing of the address distributed by the DHCP Server is not matching with the routing of the interface address.
Influence	The user in L3 interface can not obtain the IP address.

Recommended Operations	Check whether the ippool address binded by DHCP is matching with the interface address(direct-connection) and whether there is routing to the Relay agent(with relay).
Alarm Prototype Description	no match route from access interface! Alarm occurred 13:58:23 07/17/2008 UTC alarm 23818 occurred % DHCP % no match route from access interface! sent by MEC 1
Alarm Description	The routing of the address distributed by the DHCP Server is not matching with the routing of the interface address.
Supported Devices	ZXR10 3900, 5900, 6900 series switch. T64E, T128, T600, T1200 series router.

23819

Message No.	23819
Default Severity Level	6
Alarm Recovery	Unavailable
Alarm Type	ProcessingErrorAlarm
NM Level	5
Cause	The L3 interface configuring DHCP Server does not bind DHCP Policy.
Influence	The user in L3 interface can not obtain the IP address.
Recommended Operations	Check whether the L3 interface configuring DHCP Server binds DHCP Policy.
Alarm Prototype Description	Interface %s has no valid binded DHCP Policy! %s L3 interface name of DHCP user access Alarm occurred 16:57:45 07/17/2008 UTC alarm 23819 occurred % DHCP % interface vlan100 has no valid binded DHCP Policy!! sent by MEC 1
Alarm Description	The L3 interface configuring DHCP Server does not bind DHCP Policy.
Supported Devices	ZXR10 3900, 5900, 6900 series switch. T64E, T128, T600, T1200 series router.

23820

Message No.	23820
Default Severity Level	6
Alarm Recovery	Unavailable
Alarm Type	ProcessingErrorAlarm
NM Level	5

Cause	DHCP access user number reaches the upper threshold.
Influence	The user in L3 interface can not obtain the IP address.
Recommended Operations	Increase the upper threshold or advise the user to go online from other interface.
Alarm Prototype Description	user number have reached the %s's quota %u ! %s: L3 interface name %u: user quota number Alarm occurred 14:47:55 07/07/2008 UTC alarm 23820 occurred % DHCP % user number have reached t he vlan100's quota 5 ! sent by NPC 2
Alarm Description	DHCP access user number reaches the upper threshold.
Supported Devices	ZXR10 3900, 5900, 6900 series switch. T64E, T128, T600, T1200 series router.

23821

Message No.	23821
Default Severity Level	4
Alarm Recovery	Unavailable
Alarm Type	ProcessingErrorAlarm
NM Level	5
Cause	Invalid dhcppolicy.
Recommended Operations	Check whether DHCPPOLICY configuration is correct(enable DHCP-POLICY debug to obtain more detailed information).
Alarm Prototype Description	interface bound invalid dhcppolicy[%s] %s: policy name configured(policy not exist) Alarm occurred 20:15:53 08/13/2008 UTC alarm 23821 occurred % DHCP % interface bound invalid dhcppolicy [invalidPolicy] sent by UPC(RPU) 2
Alarm Description	Invalid dhcppolicy.
Supported Devices	All.

23822

Message No.	23822
Default Severity Level	4
Alarm Recovery	Unavailable
Alarm Type	ProcessingErrorAlarm
NM Level	5

Cause	Dhcppool is not configured in dhcppolicy.
Influence	Users can not get online.
Recommended Operations	Please check the DHCPPOLICY configuration(Enable DHCPPOLICY debug. DHCPPOOL debug can obtain more detailed information.).
Alarm Prototype Description	DHCP policy [%s] not bound dhcppool %s: policy name configured. DHCPPoolis not configured in dhcp-policy. Alarm occurred 20:22:09 08/13/2008 UTC alarm 23822 occurred % DHCP % DHCP policy [validPolicy] not bound dhcppool sent by UPC(RPU) 2
Alarm Description	Dhcppool is not configured in dhcppolicy.
Supported Devices	All.

23823

Message No.	23823
Default Severity Level	4
Alarm Recovery	Unavailable
Alarm Type	ProcessingErrorAlarm
NM Level	5
Cause	Ippool is not configured in dhcppool.
Influence	Users can not get online.
Recommended Operations	Please check the DHCPPOLICY configuration.(Enable DHCPPOLICY debug. DHCPPOOL debug can obtain more detailed information.)
Alarm Prototype Description	DHCP policy bound invalid dhcppool [%s] %s: dhcp pool name configured(this dhcppool not exist) Alarm occurred 20:24:35 08/13/2008 UTC alarm 23823 occurred % DHCP % DHCP policy bound invalid dhcppool [invalidPool] sent by UPC(RPU) 2
Alarm Description	Invalid dhcppool.
Supported Devices	All.

23824

Message No.	23824
Default Severity Level	4
Alarm Recovery	Unavailable
Alarm Type	ProcessingErrorAlarm
NM Level	5

Cause	Ippool is not configured in dhcppool.
Influence	Users can not get online.
Recommended Operations	Please check the DHCPPOLICY configuration.(Enable DHCPPOLICY debug. DHCPPOOL debug can obtain more detailed information.)
Alarm Prototype Description	DHCP pool [%s] not bound ippool %sdhcppool name(dhcppool not bound ippool) Alarm occurred 20:28:29 08/13/2008 UTC alarm 23824 occurred % DHCP % DHCP pool [validPool] not bound ippool sent by UPC(RPU) 2
Alarm Description	IPPool is not configured in dhcppool.
Supported Devices	All.

MLD Alarm

24064

Message No.	24064
Default Severity Level	6
Cause	MLD multicast member joins
Influence	Users can not get online.
Recommended Operations	N.A.

24065

Message No.	24065
Default Severity Level	6
Cause	MLD multicast member leaves.
Recommended Operations	Check whether MLD configuration is correct and proper. Check whether it receives MLD multicast member joining or leaving packets.

STP Alarm

24320

Message No.	24320

Default Severity Level	4
Alarm Recovery	unavailable
Alarm Type:	ProcessingErrorAlarm
NM Level	5
Cause	If configure STPLOOP protection for port instance, after running, the port instance can not receive BPDU message.
Recommended Operations	Users need to check whether there is something abnormal of the port or whether the topology is changed. If the topology is not changed, but there is something abnormal on this port, then re-boot the port please.

24321

Message No.	24321
Default Severity Level	6
Cause	Port instance configure gets rid of STPLOOP protect. Port instance is blocked formerly, but now it receives BPDU packet.
Recommended Operations	N.A.

24322

Message No.	24322
Default Severity Level	6
Cause	Configure STPROOT protect on the port instance, or the port instance receives superior BPDU packet.
Recommended Operations	Check the configuration on the switch connected with this port. Set the instance priority a little higher.

24323

Message No.	24323
Default Severity Level	6
Cause	Delete STPROOT protect on the port instance, or the port instance receives inferior BPDU packet.
Recommended Operations	N.A.

24327

Message No.	24327
Default Security Level	6

Alarm Recovery	None
Alarm Type	Communication Alarm
NM Level	5
Cause	After the rack enables STP, enables BPDU tranparent transmission.
Influence	After BDPU transparent transmission is enabled, STP can't be enabled. Other protocols need to be configured to avoid loop otherwise it will cause network storm.
Recommended Operations	It is not recommended that both STP and BPDU message transparent transmission are enabled at the same time unless special requirements.
Alarm Description Prototype	mst: spanning-tree transparent enable,please avoid boardcast storm! Example: An alarm 24323 level 6 occurred at 16:43:07 11/10/2008 UTC sent by MEC 1 %STP% mst: spanning-tree transparent enable,please avoid boardcast storm!
Alarm Description	After BDPU transparent transmission is enabled, STP can't be enabled. Other protocols need to be configured to avoid loop otherwise it will cause network storm.
Supported Devices	69/89 Switches

LOCAL ACCOUNTING Alarm

24832

Message No.	24832
Default Severity Level	6
Cause	Accounting cache of local storage exceeds alert value.
Recommended Operations	Check whether the communication between UAS and accounting server is normal.

LDP Alarm

25344

Message No.	25344
Default Severity Level	6
Cause	Two different types of pw(spoke and hub) are configured in one vfi.

Recommended Operations	Check whether the newly configured pw generates loop. If there is loop, delete this pw configuration. Otherwise, ignore this alarm.

25347

Message No.	25347
Default Severity Level	3
Alarm Recovery	Available
Alarm Type	CommunicationAlarm It is suggested that NM not show this alarm to user.
NM Level	5
Cause	LDP neighbor is down
Influence	Corresponding LSP changes to untagged and packets can't be delivered according to tag.
Recommended Operations	Check whether LDP configurations is changed and whether related direct-connect link is down.
Alarm Prototype Description	Alarm occurred LDP neighbor:%s is DOWN, pre-state: %s, state: %s,status code: %d Alarm cleared LDP neighbor: %s is UP, pre-state: %s, state: %s,status code: %d The first %s: LDP ID The second %s: the session state before this alarm. The third %s: the current session state The first %d: the reason that this alarm generates 00:01:07 01/01/2001 UTC alarm 25347 occurred %LDP neighbor:2.2.2.22:0 is down, pre-state: OPERATIONAL, state: NONEXISTENT,status code: 9 % 00:01:12 01/01/2001 UTC alarm 25347 cleared %LDP neighbor:2.2.2.22:0 is up, pre-state: OPENREC, state: OPERATIONAL,status code: 513 %
Alarm Description	LDP neighbor turns from OPERATIONAL state to NON EXIST state.
Supported Devices	ZXR10 T128.

25349

Message No.	25349
Default Severity Level	8
Cause	LDP GR is enabled

Alarm Prototype Description	Alarm occurred 00:01:07 01/01/2001 UTC alarm 25349 occurred %LDP GR%

25351

Message No.	25351
Default Severity Level	8
Cause	LDP protocol conducts the operation Clear MPLS LDP Neighbor.
Alarm Prototype Description	Alarm occurred 00:01:07 01/01/2001 UTC alarm 25351 occurred %LDP% Clear neighbor

25354

Message No.	25354
Default Severity Level	8
Cause	LDP protocol fails to operate memory, including application for memory space, release of memory and other operations.
Alarm Prototype Description	Alarm occurred 00:01:07 01/01/2001 UTC alarm 25354 occurred % LDP Memory%

25355

Message No.	25355
Default Severity Level	8
Cause	LDP protocol fails to apply timer.
Alarm Prototype Description	Alarm occured 00:01:07 01/01/2001 UTC alarm 25355 occurred % LDP Timer%

25356

Message No.	25356
Default Severity Level	8
Cause	LDP fails to apply for LABEL resources, which are insufficient.
Alarm Prototype Description	Alarm occurred 00:01:07 01/01/2001 UTC alarm 25356 occurred % LDP Label%

25357

Message No. 25357

Default Severity Level 8

Cause LDP fails to apply for FEC resources, which are insufficient.

Alarm Prototype Description Alarm occurred

00:01:07 01/01/2001 UTC alarm 25357 occurred % LDP Fec%

L2VPN Alarms

25856

Message No. 25856

Default Severity Level 6

Cause MAC address learned from VPLS changes. E.g. MAC migrates from one port to another port.

25857

Message No. 25857

Default Severity Level 8

Cause TLV is unknown to L2VPN

Alarm ProtoType Description Alarm occurred

00:01:07 01/01/2001 UTC alarm 25857 occurred %L2VPN% Unknown L2VPN TLV

25858

Message No. 25858

Default Severity Level 8

Cause GR is enabled in L2VPN

Alarm ProtoType Description Alarm occurred

00:01:07 01/01/2001 UTC alarm 25858 occurred %L2VPN GR%

25859

Message No. 25859

Default Severity Level	8
Cause	L2VPN VC resources are insufficient
Alarm ProtoType Description	Alarm occurred 00:01:07 01/01/2001 UTC alarm 25858 occurred %L2VPN GR%

25863

Message No.	25863
Default Severity Level	8
Cause	It fails to operate L2VPN timer.
Alarm ProtoType Description	Alarm occurred 00:01:07 01/01/2001 UTC alarm 25863 occurred %L2VPN Timer%

25864

Message No.	25864
Default Severity Level	8
Cause	L2VPN LABEL resources are insufficient.
Alarm ProtoType Description	Alarm occurred 00:01:07 01/01/2001 UTC alarm 25864 occurred %L2VPN% Label

ZESR Alarms

26368

Message No.	26368
Default Severity Level	6
Cause	ZESR ring turns from down state to up state.
Recommended Operations	It notifies state changes of ZESR master node.

26369

Message No.	26369
Default Severity Level	6
Cause	ZESR ring turns from down state to preup state.

Recommended Operations	It notifies state changes of ZESR master node.

26370

Message No.	26370
Default Severity Level	6
Cause	ZESR ring turns from up state to down state and the reason is that Hello packet times out.
Recommended Operations	It notifies state changes of ZESR master node.

26371

Message No.	26371
Default Severity Level	6
Cause	ZESR ring turns from up state to down state and the reason is that Link-down frame is received.
Recommended Operations	It notifies state changes of ZESR master node.

26372

Message No.	26372
Default Severity Level	6
Cause	ZESR ring turns from preup state to down state and the reason is that Hello packet times out.
Recommended Operations	It notifies state changes of ZESR master node.

26373

Message No.	26373
Default Severity Level	6
Cause	ZESR ring turns from preup state to down state and the reason is that Link-down frame is received.
Recommended Operations	It notifies state changes of ZESR master node.

26374

Message No.	26374
Default Severity Level	6
Cause	ZESR ring turns from preup state to up state.

Recommended Operations It notifies state changes of ZESR master node.

26375

Message No. 26375

Default Severity Level 6

Cause ZESR ring turns from down state to up state.

Recommended Operations It notifies state changes of ZESR master node.

26376

Message No. 26376

Default Severity Level 6

Cause ZESR ring turns from up state to down state.

Recommended Operations It notifies state changes of ZESR master node.

TACACS Alarms

28160

Message No. 28160

Default Severity Level 5

Cause Tacacs+ client authentication queue is full.

Recommended Operations Please check whether the configuration of tacacs+server is correct; whether AAA configuration on NAS is correct; whether interconnection between NAS and server is ok; whether network communication is normal.

28161

Message No. 28161

Default Severity Level 5

Cause Tacacs+ client authorization queue is full.

Recommended Operations Please check whether the configuration of tacacs+server is correct; whether AAA configuration on NAS is correct; whether interconnection between NAS and server is ok; whether network communication is normal.

28162

Message No. 28162

Default Severity Level 5

Cause Tacacs+ client accounting queue is full.

Recommended Operations Please check whether the configuration of tacacs+server is correct; whether AAA configuration on NAS is correct; whether interconnection between NAS and server is ok; whether network communication is normal.

28163

Message No. 28163s

Default Severity Level 5

Cause Invalid packet is received from tacacs+ server.

Recommended Operations Please check whether the configuration of tacacs+server is correct; whether AAA configuration on NAS is correct; whether shared keys configured on them are identical.

28164

Message No. 28164

Default Severity Level 5

Cause Tacacs+ functional module is not enabled.

Recommended Operations Please enable tacacs+ function.

28165

Message No. 28165

Default Severity Level 5

Cause There is no server available in Tacacs+ server group.

Recommended Operations Please check whether the configuration of tacacs+server is correct; whether AAA configuration on NAS is correct; whether interconnection between NAS and server is ok; whether network communication is normal.

28166

Message No. 28166

Default Severity Level 5

Cause The size of Tacacs+ request packet is overlarge.

Recommended Operations Please modify the max size of tacacs+ packet, disable tacacs+ function and re-enable tacacs+.

28167

Message No. 28167

Default Severity Level 4

Cause Tacacs+ authentication request is wrong.

Recommended Operations It's an internal error, and please contact ZTE engineer.

28168

Message No. 28168

Default Severity Level 6

Cause Tacacs+ request packet is timeout.

Recommended Operations Please check whether the configuration of tacacs+server is correct; whether AAA configuration on NAS is correct,; whether interconnection between NAS and server is ok; whether network communication is normal.

28169

Message No. 28169

Default Severity Level 6

Cause The authentication type is not supported by NAS client.

Recommended Operations NAS doesn't support authentication of ARAP type.

AAA Alarms

28418

Message No. 28418

Default Severity Level 5

Cause The used AAA method is not defined.

Recommended Operations Please check whether AAA method name is wrong or define a new AAA method list.

28419

Message No. 28419

Default Severity Level 5

Cause The type of AAA method list is wrong.

Recommended Operations Please use the correct AAA method list configured for the service type.

28421

Message No. 28421

Default Severity Level 5

Cause The specified server group is not defined.

Recommended Operations Please check whether server group is correct or define this server group.

28422

Message No. 28422

Default Severity Level 5

Cause Server members are not configured in server group.

Recommended Operations Please configure at least one member for the server group.

28423

Message No. 28423

Default Severity Level 5

Cause NAS detects an unknown attribute.

Recommended Operations Please check whether the server configuration attribute-value pair is wrong and whether the attribute-value pair is supported by NAS.

28429

Message No. 28429

Default Severity Level 5

Cause AAA fails to apply for memory space.

Recommended Operations Please check whether system memory utilization reaches the max and whether system configuration information reaches or exceeds the threshold; if it does, consider upgrading the device. If system

memory utilization doesn't reach the max, please contact ZTE engineer.

MIX Alarms

29952

Message No. 29952

Default Severity Level 3

Cause If the alarm state is occurred, it indicates the alarm has occurred.

The general reason is main board detects that communication with other card breaks and the card doesn't work;

In case alarm state is Cleared, it indicates the alarm has been cleared.

The general reason is main board detects that communication with other card is ok and the card works normally.

Recommended Operations In case alarm state is Occurred, please check if this card works normally.

Alarm ProtoType Description Alarm occurred

10:12:57 09/15/2006 UPC alarm 29952 occurred. Mp check np 1: communication failed! sent by UPC 1

Alarm cleared

10:12:59 09/15/2006 UTC alarm 29952 cleared. Mp check np 1: communication succeeded! sentbyUPC1

29953

Message No. 29953

Default Severity Level 6

Cause In case alarm state is Occurred, it indicates the alarm has occurred. Generally, the reason is router is attacked by TCP SYN Flood.

Alarm ProtoType Description Alarm occurred

00:00:12 01/01/2001 UTC alarm 29953 occurred %MIX% The router is attacked by tcp syn flood! sent by MCP

29954

Message No. 29954

Default Severity Level 6

Cause	In case alarm state is Occurred, it indicates that an alarm has occurred and generally the reason is TCP SYN Waittime changes.
Alarm ProtoType Description	Alarm occurred 00:00:12 01/01/2001 UTC alarm 29954 occurred %MIX% TCP SYNWAIT time is changed for defending syn flood attacking! sent by MCP

29955

Message No.	29955
Default Severity Level	6
Cause	In case alarm state is Occurred, it indicates that an alarm has occurred and generally the reason is TCP SYN Waittime restores to the original value.
Alarm ProtoType Description	Alarm occurred 00:00:11 01/01/2001 UTC alarm 29955 occurred %MIX% TCP SYNWAIT time is recovered! sent by MCP

29956

Message No.	29956
Default Severity Level	5
Alarm Recovery	Available
Alarm Type	QoSAlarm
NM Level	4
Cause	Alarm occurred The received packet in per unit time is more than the set value. The command used to set the value is: ZXR10(config-if)#port-up-send limit[packets num receive-interval num close-interval num]. The mode is interfasce configure mode, the received packet is counted by number and the time unit is seconds. By default, to receive 20 packets costing 2 seconds. Alarm cleared Recover automatically when the set closing time is over. The configure mode and the value is the same as the above. The time unit is minutes, it is 5 minutes by default.
Influence	The current port receives much more packets and the port is closed. After a while, the port opens automatically. The default waiting time is 5 minutes.
Recommended Operations	Reduce system load.
Alarm Prototype Description	\nPort 0x%x CPU Protect Port Upsend Close\nPort 0x%x Cpu Protect Port Upsend Open 0x%x is the global port number of the interface

05:42:40 04/20/2001 UTC alarm 29956 cleared %MIX% Port 0x7 Cpu Protect Port Upsend Open on fei_4/3 sent by NPC 4

05:44:30 04/20/2001 UTC alarm 29956 occurred %MIX% Port 0x7 Cpu Protect Port Upsend Close on fei_4/3 sent by NPC 4

Alarm Description The packets received by the port exceed the alarm value and the port shuts down. The default alarm value is 20 packets in 2 seconds.

Supported Devices T128/T64, T600/T1200

Appendix Specification N.A.

29957

Message No. 29957

Default Severity Level 6

Alarm Recovery Available

Alarm Type ProcessingErrorAlarm

NM Level 5

Cause When the system restores the relative sub event to the event list, the event list has been deleted. Alarm occurs when plugging in the NPC again.

Recommended Operations It is a prompt. There is no need to care about it.

Alarm Prototype Description "Add entry failed, event list [%s] has been deleted".

%s: event list name.

Alarm occurred

An alarm 29957 level 6 occurred at 00:08:59 01/01/2001 UTC sent by UPC(MPU) %MIX% Add entry failed, event list [myEvent] has been deleted

Alarm Description When the system restores the relative sub event to the event list, the event list has been deleted.

Supported Devices G-series, ZXR 10 6900/8900.

Appendix Specification N.A.

29958

Message No. 29958

Default Severity Level 6

Alarm Recovery Available

Alarm Type ProcessingErrorAlarm

NM Level 5

Cause This alarm may occur when plugging in or plugging out NPC. When plugging NPC, the event total number already reaches the upper threshold. After plugging in NPC, it tries to restore interface re-

	lated sub event list. Now the member number is full and this alarm appears.
Recommended Operations	It is a prompt. There is no need to care about it.
Alarm Prototype Description	"Add entry failed, event list [%s] has too many items" %s: event list name. Alarm occurred An alarm 29958 level 6 occurred at 00:08:59 01/01/2001 UTC sent by UPC(MPU) %MIX% Add entry failed, event list [myEvent] has too many items
Alarm Description	When the system restore the relative sub event to the event list, the event total number already reaches the upper threshold.
Supported Devices	ZT600/T1200

29959

Message No.	29959
Default Severity Level	6
Alarm Recovery	Available
Alarm Type	ProcessingErrorAlarm
NM Level	5
Cause	This alarm may occur when plugging in or plugging out NPC. When plugging NPC, because other event list member is configured, the event total number already reaches the upper threshold. After plugging in NPC, it tries to restore interface related sub event list. Now the member number is full and this alarm appears.
Recommended Operations	It is a prompt. There is no need to care about it.
Alarm Prototype Description	"Add entry failed, too many event items" %s: event list name. Alarm occurred An alarm 29959 level 6 occurred at 00:08:59 01/01/2001 UTC sent by UPC(MPU) %MIX% Add entry failed, too many event items
Alarm Description	When the system restore the relative sub event to the event list, the event total number already reaches the upper threshold.
Supported Devices	G-series, ZXR10 6900/8900.

29960

Message No.	29960
Default Security Level	5
Alarm Type	"ProcessingErrorAlarm"
NM Level	5

Cause The number that netflow configures on the line card exceeds the upper limit specified by system.

The command of sampling rate of configured interface is :**netf low-sample-rate** { **ingress** | **egress**}{ **unicast** | **multicast**| **mpls** |{ **aacll** < *acl name*>}}< *1~65535*> , at global configuration mode.

Influence The sampling configuration that exceeds threshold number can't take effect.

Recommended Operations Delete the Netflow sample configuration that exceeds the limit.

Use the **no netflow-sample-rate** { **ingress** | **egress**}{ **unicast** | **multicast**| **mpls** |{ **aacll** < *acl name*>}} command to delete configuration of interface.

Alarm Description Prototype %s(M) panel %d the number of netflow configuration exceeds the limit

%s(S) panel %d the number of netflow configuration exceeds the limit

The first %s: cpu typethe first %d: panel number

Example:

An alarm 29960 level 4 occurred at 09:44:55 11/29/2008 UTC sent by NPC 2 %MIX% The number of netflow configuration exceeds the limit

Alarm Description The number that netflow configures on the line card exceeds the upper limit specified by system.

Supported Devices T128T1200 (This alarm can be available from V4.8.22.)

BFD alarm

30208

Message No. 30208

Default Severity Level 5

Cause The upper-layer application asks for establishing BFD session. It is the prompt when BFD requests the connection.

Recommended Operations It is a prompt. There is no need to care about it.

Alarm Prototype Description BFD application prompt for LDP LSP:

00:02:16 02/08/2002 UTC alarm 30208 occurred %BFD% Session [LDP BFD For FEC 10.40.64.121] is CONNECT on interface fei_1/1

BFD application prompt for RSVP LSP:

00:02:16 02/08/2002 UTC alarm 30208 occurred %BFD% Session [RSVP BFD For tunnel1] is CONNECT on interface fei_1/1

The prompt for other application:

00:02:16 02/08/2002 UTC alarm 30208 occurred %BFD% Session [10.40.64.120-->10.40.64.121] is CONNECT on interface fei_1/1

Alarm Description When the system restore the relative sub event to the event list, the event total number already reaches the upper threshold.

Supported Devices G-series, ZXR10 6900/8900.

30209

Message No. 30209

Default Severity Level 5

Cause BFD session is established and the state machine changes to UP.

Recommended Operations It is a prompt. There is no need to care about it.

Alarm Prototype Description BFD application prompt for LDP LSP:

00:02:16 02/08/2002 UTC alarm 30209 occurred %BFD% Session [LDP BFD For FEC 10.40.64.121] is UP on interface fei_1/1

BFD application prompt for RSVP LSP:

00:02:16 02/08/2002 UTC alarm 30208 occurred %BFD% Session [RSVP BFD For tunnel1] is UP on interface fei_1/1

The prompt for other application:

00:02:16 02/08/2002 UTC alarm 30208 occurred %BFD% Session [10.40.64.120-->10.40.64.121] is UP on interface fei_1/1

30210

Message No. 30210

Default Severity Level 5

Cause BFD session is established and the state machine changes to DOWN.

Recommended Operations It is a prompt. There is no need to care about it.

Alarm Prototype Description BFD application prompt for LDP LSP:

00:02:16 02/08/2002 UTC alarm 30209 occurred %BFD% Session [LDP BFD For FEC 10.40.64.121] is DOWN on interface fei_1/1

BFD application prompt for RSVP LSP:

00:02:16 02/08/2002 UTC alarm 30208 occurred %BFD% Session [RSVP BFD For tunnel1] is DOWN on interface fei_1/1

The prompt for other application:

00:02:16 02/08/2002 UTC alarm 30208 occurred %BFD% Session [10.40.64.120-->10.40.64.121] is DOWN on interface fei_1/1

30212

Message No.	30212
Default Severity Level	5
Cause	When BFD conversation is created, the number of conversation on a CPU exceeds the limit.
Alarm Prototype Description	When establishing session, a prompt on RP is as follows: 00:02:16 02/08/2002 UTC alarm 30212 occurred %BFD% RPU create too many Sessions When establishing session, a prompt on NP is as follows: 00:02:16 02/08/2002 UTC alarm 30212 occurred %BFD% NPC Panel 1 create too many Sessions

30213

Message No.	30213
Default Security Level	5
Alarm Type	"ProcessingErrorAlarm"
NM Level	5
Cause	Establish BFD session on the interface which doesn't support it. The current switch supports VLAN, SUPERVLAN interface. The high-end router supports the following interfaces: it,ge4c,xgel,xgew,vlan-geit,vlan-ge4c,vlan-xgel,vlanxgew, qinq-geit,qinq-ge4c,qinq-xgel,qinq-xgew,P48F,P192,Feig,Feiog,ge4b,ge4d,vlanfeig, vlan-feigo,vlan-ge4b,vlan-ge4d,qinq-feig,qinq-feigo,qinq-ge4b,qinqge4d, p3c,p12,p48,cp3,A3c,A3D,A12.
Influence	BFD session can't be established.
Recommended Operations	Please establish BFD session on the interface supporting it.
Alarm Description Prototype	Session CANNOT be created on interface %s. %sindicate interface name. Example: An alarm 30213 level 5 occurred at 00:07:31 01/01/2001 UTC sent by UPC(RPU) 1 %BFD% Session CANNOT be created on interface smartgroup1
Alarm Description	Establish BFD session on the interface which doesn't support it.

Supported Devices All series

UDLD Alarm

29696

Message No. 29696

Default Severity Level 5

Alarm Type EnvironmentalAlarm

NM Level 5

Cause The neighbourhood is established between UDLD port and this port.

Recommended Operation Check whether there is self-loop in the port. If self-loop exists, check whether it is necessary to remove the self-loop.

Alarm Prototype Description interface build udld neighbour with itself on %s

%s: interface name

00:01:28 01/01/2001 UTC alarm 29696 occurred %UDLD% interface build udld neighbour with itself on gei_1/25 sent by MCP

Supported Device ZXR10 3900/6900.

29697

Message No. 29697

Default Severity Level 5

Alarm Type EnvironmentalAlarm

NM Level 5

Cause The neighbourhood is established between two ports on this device.

Recommended Operation Check whether there is loop in the port. If loop exists, check whether it is necessary to remove the loop.

Alarm Prototype Description interface %s and %s build udld neighbour relationship

%s: interface name, the two interfaces connect with the rack directly.

00:14:07 01/01/2001 UTC alarm 29697 occurred interface fei_1/2 and fei_1/8 build udld neighbour relationship sent by MCP

Alarm Description The loop occurs between the two ports.

Supported Device ZXR10 3900/6900.

29698

Message No.	29698
Default Severity Level	4
Alarm Recovery	Unavailable.
Alarm Type	CommunicationAlarm
NM Level	4
Cause	All the neighbourhood is removed.
Influence	All the neighborhood is lost on this port. If this interface is in UDLDAggressive mode, it will activate the neighborhood detection. If this interface can not be detected, the link is regarded as monologue and sets this interface DOWN.
Recommended Operation	Check whether the communication between this port and the other port is normal.
Alarm Prototype Description	all neighbours clear on %s %s: interface name 00:28:40 01/01/2001 UTC alarm 29698 occurred all neighbours clear on fei_1/2 sent by MCP
Alarm Description	All the neighbourhood is removed. No UDLD HELLO packet is from the other end.
Supported Device	ZXR10 3900/6900.

29699

Message No.	29699
Default Severity Level	3
Alarm Recovery	Available.
Alarm Type	CommunicationAlarm
NM Level	3
Cause	1. When the interface is under Aggressive mode, all the neighbor is aging. 2. Optical interface: The sending and receiving optical fibres connect two different interfaces.
Influence	Sets the interface state to err-disable. No protocol is running under this interface.
Recommended Operation	Check immediately whether the link connection between this port and the other port is normal.
Alarm Prototype Description	interface unidirection occurs on %s %s: interface name 00:28:48 01/01/2001 UTC alarm 29699 occurred interface unidirection occurs on fei_1/2 sent by MCP 00:03:17 01/01/2001 UTC alarm 29699 cleared %UDLD% interface unidirection clears on fei_1/2 sent by MCP

Alarm Description	Monologue occurs in the port
Supported Device	ZXR10 3900/6900.

MUX Alarm

29440

Message No.	29440
Default Severity Level	6
Cause	Please add protocol packet test function on high-end switch. Give alarms to remind users for the abnormal protocol packet.
Recommended Operation	Please check whether the network condition is correct, suitable. If there is no problem of the configuration, please copy the info and contact ZTE's maintenance personnel.
Alarm Prototype Description	Alarm occured: 10:55:05 03/29/2007 UTC alarm 22793 occurred %MAC%<MAC Table> mode in micode-learning,please input mac learn special sent by MEC 1
Alarm Description	The original alarm message number is 21768.

ZESS Alarm

32512

Message No.	32512
Default Severity Level	6
Alarm Recovery	Available
Alarm Type	Equipment Alarm
NM Level	4
Cause	ZESS link state turns from UP to DOWN.
Recommended Operations	N.A.
Alarm Prototype Description	Domain %u from down to up Domain %u from up to down %d: the area id number, it can be 1-4. An alarm 32512 level 5 occurred at 04:49:42 02/01/2001 UTC sent by NPC 2 %ZESS% Domain 1 from down to up

	An alarm 32512 level 5 cleared at 04:49:42 02/01/2001 UTC sent by NPC 2 %ZESS% Domain 1 from up to down
Alarm Description	ZESS link state is DOWN.
Supported Devices	ZXR10 T40 T64 T160.
Appendix Specification	N.A.

32513

Message No.	32513
Default Severity Level	6
Alarm Recovery	Unavailable
Alarm Type	Equipment Alarm
NM Level	5
Cause	During ZESS link state recovery, the link is in PREUP state that is a transition from DOWN to UP.
Recommended Operations	N.A.
Alarm Prototype Description	Domain %u from down to preup %d: the area id number, it can be 1-4. An alarm 32513 level 5 occurred at 04:49:42 02/01/2001 UTC sent by NPC 2 %ZESS% Domain 1 from down to preup
Alarm Description	ZESS is in a preup state when the link state recovers.
Supported Devices	ZXR10 T40 T64 T160.
Appendix Specification	N.A.

32514

Message No.	32514
Default Severity Level	6
Alarm Recovery	Unavailable
Alarm Type	Equipment Alarm
NM Level	5
Cause	The timer times out. ZESS state turns from PREUP to UP.
Recommended Operations	N.A.
Alarm Prototype Description	Domain %u from preup to up %u: area id, it can be 1-4. An alarm 32514 level 5 occurred at 04:49:42 02/01/2001 UTC sent by NPC 2 %ZESS% Domain 1 from preup to up
Alarm Description	The timer times out. ZESS state turns from PREUP to UP.
Supported Devices	ZXR10 T40 T64 T160.

Appendix Specification N.A.

POE Alarm

30720

Message No. 30720

Default Security Level 6

Alarm Recovery None

Alarm Type SoftProtocolAlarm

NM Level 5

Cause PSE disables POE function because of over-temperature on the switch; PSE recovers POE function because of temperature recovers; PSE total power of the power supply exceeds power threshold or recovers in the range of power threshold.

Influence Cancel POE function due to high temperature; PSE is made not to supply power because the total power of the power supply exceeds power threshold.

Recommended Operations Check if the temperature of environment where switch is in is too high.

Alarm Description Prototype Disable POE function because that the whole PSE is over-temperature on the switch.

Disable poe function of the pse %d because of over-temperature on the switch

Example:

09:40:10 11/13/2008 UTC alarm 30721 occurred %POE% Disable poe function of the pse 1 because of over-temperature on the switch sent by MEC 1

PSE total power of the power supply exceeds power threshold or recovers in the range of power threshold.

The usage power (%dw) is below the PSE threshold (%dw) on pse %d

The first %d: PSE total power of the power supply

The second %d: PSE power threshold.

The third %d: PSE device number.

The usage power (%dw) is above the PSE threshold (%dw) on pse %d

The first %d: PSE total power of the power supply

The second %d: PSE power threshold.

The third %d: PSE device number.

Example:

19:38:23 06/19/2006 UTC alarm 30720 occurred %POE% The usage power (0w) is below the PSE threshold (30w) on pse 1 sent by MCP

Alarm Description

1. PSE disables POE function because of over-temperature on the switch.
2. PSE total power of the power supply recovers in the range of power threshold.

Supported Devices ZXR10 3928A-PS ZXR10 5928-PS

30721

Message No. 30721

Default Security Level 6

Alarm Recovery None

Alarm Type SoftProtocolAlarm

NM Level 5

Cause no response from port, no response from chip, no response from firmware, overload. Device abnormality causes that POE port power supply is cancelled.

Influence POE function on the port is invalid and power supply is disabled.

Recommended Operations Check device according to the prompt.

Alarm Description Prototype

POE on the port is disabled.

PoE disable (for no response from port)

Example:

09:40:10 11/13/2008 UTC alarm 30720 occurred %POE% PoE disable (for no response from port) on gei_2/1/24 sent by MEC 1

The port power supply status is changing.

The PSE power detection status is searching

The PSE power detection status is deliveringPower

Example2:

17:52:09 06/19/2006 UTC alarm 30721 occurred %POE% The PSE power detection status is deliveringPower on gei_1/10 sent by MCP

Alarm Description

1. Power supply function on gei_2/1/24 is cancelled because of no response from port.
2. The power supply status on gei_1/10 becomes being in power supply.

Supported Devices ZXR10 3928A-PS ZXR10 5928-PS

ESM Alarm

26385

Message No. 26385

Default Security Level 6

Alarm Recovery None

Alarm Type Communication Alarm

NM Level 5

Cause After device or board is restarted, if MP detects that ESM configuration of line card is different from the local one MP will download ESM configuration on line card and save it.The ESM configuration will be valid when line card is restarted.

Recommended Operations Restart the specific board according to alarm message.

Alarm Description Prototype MP had sent configration to slot 1 and set successfully!!! Please reload slot 1!!!

Example:

08:50:51 09/04/2009 UTC alarm 26385 occurred MP had sent configration to slot 1 and set successfully!!! Please reload slot 1!!! sent by MEC 1

Alarm Description If MP detects that ESM configuration of line card is different from the local one MP will download ESM configuration on line card and save it.The ESM configuration will be valid when line card is restarted.

Supported Devices 69/89 Switches

EPON Alarm

33280

Message No. 33280

Default Security Level 5

Alarm Type "CommunicationAlarm"

NM Level 5

Cause Because the attenuation of the optical path between ONU and OLT is out of normal range or ONU and OLT optical parameter config-

urations are not correct , optical path is abnormal and the data transmission abnormality occurs on bit.

Influence The transmission data is abnormal.

Recommended Operations Check the fiber connection between ONU module and OLT module.

This alarm is called bit error rate alarm in EPON project. This alarm can be opened and closed by using command and set alarm switch, alarm monitor direction and alarm threshold. In default, this alarm is enabled and the monitor direction is up-down-link, the value is 10(unit:10^{-9}). If the alarm need to be closed configure "alarm bit-error-rate disable " on OLT interface. If the monitor direction and threshold need to be modified configure the command **alarm bit-error-rate direction** < *direction*> **tthrressholld** < *thresho ld*> on the OLT interface.

Alarm Description Prototype "Epon alarm bit-error-rate occour at %d in %s direction!"

%dindicate bit-error-rate value when alarm occurs.

%sindicate the monitor direction when bit-error-rate alarm occurs.

The monitor directions are as follows:

uplinkindicate monitor directiononly monitor the uplink communication data forwarded from ONU to OLT.

downlinkindicate monitor directiononly monitor the downlink communication data forwarded from ONU to OLT.

up-down-link indicate monitor direction monitor the uplink and downlink communication data forwarded from ONU to OLT.

Example:

18:57:30 08/26/2008 UTC alarm 33280 occurred %EPON% Epon alarm bit-error-rate occour at 100000 in uplink direction! sent by NPC 3

Alarm Description Bit error occurs in communication between ONU module and OLT module.

Supported Devices EPON project of 4822

33281

Message No. 33281

Default Security Level 5

Alarm Type "CommunicationAlarm"

NM Level 5

Cause Because the attenuation of the optical path between ONU and OLT is out of normal range or ONU and OLT optical parameter configurations are not correct , optical path is abnormal and the data frame transmission is abnormal .

Influence The transmission data is abnormal.

Recommended Operations Check the fiber connection between ONU module and OLT module.

This alarm is called frame error rate alarm in EPON project. This alarm can be opened and closed by using command and set alarm

	switch, alarm monitor direction and alarm threshold. In default, this alarm is enabled and the monitor direction is up-down-link, the value is 1(unit:10^{-9}). If the alarm need to be closed configure "alarm frame error- rate disable"on OLT interface. If the monitor direction and threshold need to be modified configure the command **alarm frame-error-rate direction** < *direction*> **tthrr essholld** < *threshold*> on the OLT interface.
Alarm Description Prototype	"Epon alarm frame-error-rate occour at %d in %s direction!" %dindicate frame-error-rat value when alarm occurs. %sindicate the monitor direction when frame-error-rat alarm occurs. The monitor directions are as follows: uplinkindicate monitor directiononly monitor the uplink communication data forwarded from ONU to OLT. downlinkindicate monitor directiononly monitor the downlink communication data forwarded from ONU to OLT. up-down-link indicate monitor direction monitor the uplink and downlink communication data forwarded from ONU to OLT. Example: 18:57:30 08/26/2008 UTC alarm 33281 occurred %EPON% Epon alarm frame-error-rate occour at 1000 in up-down-link direction! sent by NPC 3
Alarm Description	Frame error occurs in communication between ONU module and OLT module.
Supported Devices	EPON project of 4822

33282

Message No.	33282
Default Security Level	5
Alarm Type	"CommunicationAlarm"
NM Level	5
Cause	Time-slot is wrong and ONU module doesn't forward packets in its own time-slot.
Influence	ONU forwards data abnormally.
Recommended Operations	Check time-slot on ONU module. This alarm is called llid-mismatch alarm in EPON project. In default, this alarm is disabled and LLID matching fault frame threshold is 5000 frames. If the alarm need to be enabled configure "alarm llid-mismatch enable"on OLT interface. If the alarm threshold need to be modified configure the command **alarm llid-mism atch threshold** < *threshold*> on the OLT interface.
Alarm Description Prototype	"Epon alarm llid-mismatch occour at %d!" %dindicate llid-mismatch value when alarm occurs. Example:

	18:57:30 08/26/2008 UTC alarm 33282 occurred %EPON% Epon alarm llid-mismatch occour at 6000! sent by NPC 3
Alarm Description	Time-slot is wrong and ONU module doesn't forward packets in its own time-slot.
Supported Devices	EPON project of 4822

33283

Message No.	33283
Default Security Level	5
Alarm Type	"CommunicationAlarm"
NM Level	5
Cause	Detect on local OLT: system mixes ONU version . For example, use ONU with OAM1.2 and ONU with OAM 2.0 together (because ONU must apply the same OAM version in the same system).
Influence	Optical path is abnormal.
Recommended Operations	Provide the same version for the two ONU modules. This alarm is called local-stable alarm in EPON project. In default, this alarm is enabled. If the alarm need to be disabled configure "alarm local-stable disable" on OLT interface.
Alarm Description Prototype	"Epon alarm local-stable occour!" Example: 14:57:30 08/26/2008 UTC alarm 33283 occurred %EPON% Epon alarm local-stable occour! sent by NPC 3
Alarm Description	Detect on local OLT: system mixes ONU version .
Supported Devices	EPON project of 4822

33284

Message No.	33284
Default Security Level	5
Alarm Type	"CommunicationAlarm"
NM Level	5
Cause	Detect on remote OLT: system mixes ONU version . For example, use ONU with OAM1.2 and ONU with OAM 2.0 together (because ONU must apply the same OAM version in the same system).
Influence	Optical path is abnormal.
Recommended Operations	Provide the same version for the two ONU modules. This alarm is called remote stable alarm in EPON project. In default, this alarm is enabled. If the alarm need to be disabled configure "alarm remote-stable disable" on OLT interface. This alarm generates on ONU side and be sent back to OLT.

Alarm Description Prototype	"Epon alarm remote-stable occour!" Example: 15:52:30 08/26/2008 UTC alarm 33284 occurred %EPON% Epon alarm remote-stable occour! sent by NPC 3
Alarm Description	Detect on remote OLT: system mixes ONU version .
Supported Devices	EPON project of 4822

33285

Message No.	33285
Default Security Level	5
Alarm Type	"CommunicationAlarm"
NM Level	5
Cause	When ONU shouldn't change encryption-key (encryption-key is the key that generates randomly in ONU discovery process and used to encrypt and decrypt the data forwarded from ONU to OLT), it changes.
Influence	Optical path is abnormal.
Recommended Operations	Disconect, re-connect, and register ONU. This alarm is called bad encryption key alarm in EPON project. In default, this alarm is enabled. If the alarm need to be disabled configure "alarm bad-encryption-key disable" on OLT interface.
Alarm Description Prototype	"Epon alarm bad-encryption-key occour!" Example: 18:57:23 08/26/2008 UTC alarm 33285 occurred %EPON% Epon alarm bad-encryption-key occour! sent by NPC 3
Alarm Description	ONU encryption-key changes.
Supported Devices	EPON project of 4822

33286

Message No.	33286
Default Security Level	5
Alarm Type	"CommunicationAlarm"
NM Level	5
Cause	The fault occurs in ONU registration process.
Influence	ONU fails to register.
Recommended Operations	Register ONU again. This alarm is called registration error alarm in EPON project. In default, this alarm is enabled. If the alarm need to be disabled configure "alarm registration-error disable" on OLT interface.

ONU registration command examples (**<***slot*> is the slot number of epon single board).

1. The registration that doesn't need binding mac.
   i. **hardware-authentication card** <*slot*>**disabled**
   ii. **auto-authentication card** <*slot*>**enable**
2. The registration that need binding mac.
   i. **hardware-authentication card** <*slot*>**enable**
   ii. **auto-authentication card** <*slot*>**disabled**
   iii. **onu** <*onuid*> **type** <*type-name*> **mac** <*macAddr*>

Parameter description:

Parameter	Description	Range
onuid	ONU ID	1~32
type type-name	ONU model name	ZTE-D400 ZTE-D402 ZTE-D420 ZTE-D421 ZTE-D422 ZTE-F401 ZTE-F425 ZTE-F429 ZTE-F430 ZTE-F435 ZTE-F500 ZTE-F820
mac macAddr	ONU MAC address	-

Example: if epon single board is in slot 5

1. The registration that doesn't need binding mac.

```
ZXR10(config-epon)#hardware-authentication card 5 disabled
ZXR10(config-epon)#auto-authentication card 5 enable
```

2. The registration that need binding mac.

```
ZXR10(config-epon)#hardware-authentication card 5 enable
ZXR10(config-epon)#auto-authentication card 5 disabled
ZXR10(config-if)#onu 1 type ZTE-F425 mac 0015.eba3.c6c9
```

Alarm Description Prototype "Epon alarm onu registration-error occour!"

Example:

18:41:30 08/26/2008 UTC alarm 33286 occurred %EPON% Epon alarm registration-error occour! sent by NPC 3

Alarm Description ONU fails to register.

Supported Devices EPON project of 4822

33287

Message No. 33287

Default Security Level 5

Alarm Type "CommunicationAlarm"

NM Level 4

Cause	OAM link is disconnected.
Influence	OAM link is disconnected and can't connect ONU.
Recommended Operations	Check OAM link state, disconnect and re-connect ONU, or reboot the entire rack. This alarm is called oam link disconnection alarm in EPON project. In default, this alarm is enabled. If the alarm need to be disabled configure "alarm oam-link-disconnection disable" on OLT interface.
Alarm Description Prototype	"Epon alarm oam-link-disconnection occour!" Example: 18:41:30 08/26/2008 UTC alarm 33287 occurred %EPON% Epon alarm oam-link-disconnection occour! sent by NPC 3
Alarm Description	OAM link is disconnected.
Supported Devices	EPON project of 4822

33288

Message No.	33288
Default Security Level	5
Alarm Type	"CommunicationAlarm"
NM Level	4
Cause	Data loading fault or other dying gasp fault.
Influence	The optical path is abnormal.
Related Alarms	33290
Recommended Operations	Disconnect and re-connect the connection between ONU and OLT. Register ONU again. This alarm is called dying gasp alarm in EPON project. In default, this alarm is enabled. If the alarm need to be disabled configure "alarm dying-gasp disable" on OLT interface.
Alarm Description Prototype	"Epon alarm dying-gasp occour!" Example: 14:57:30 08/26/2008 UTC alarm 33288 occurred %EPON% Epon alarm dying-gasp occour! sent by NPC 3
Alarm Description	Communication over fiber is abnormal.
Supported Devices	EPON project of 4822

33289

Message No.	33289
Default Security Level	5
Alarm Type	"CommunicationAlarm"

NM Level	4
Cause	Fault occurs on the link in receive direction of local data terminal device.
Influence	Local receiving device is abnormal.
Related Alarms	33290
Recommended Operations	Check the link in receive direction of local data terminal device. This alarm is called local link fault alarm in EPON project. In default, this alarm is enabled. If the alarm need to be disabled configure "alarm local-link-fault disable" on OLT interface.
Alarm Description Prototype	"Epon alarm local-link-fault occour!" Example: 14:57:30 08/26/2008 UTC alarm 33289 occurred %EPON% Epon alarm local-link-fault occour! sent by NPC 3
Alarm Description	Fault occurs on the link in receive direction of EPON local data terminal device.
Supported Devices	EPON project of 4822

33290

Message No.	33290
Default Security Level	5
Alarm Type	"CommunicationAlarm"
NM Level	4
Cause	It's a data loading fault or other dying gasp fault. Or fault occurs in receive direction of local data terminal device.
Influence	The optical path is abnormal.
Related Alarms	33288 33289
Recommended Operations	Disconnect and re-connect the connection between ONU and OLT. Register ONU again. This alarm is called critical event alarm in EPON project. In default, this alarm is enabled. If the alarm need to be disabled configure "alarm critical-event disable" on OLT interface.
Alarm Description Prototype	"Epon alarm critical-event occour!" Example: 14:57:30 08/26/2008 UTC alarm 33290 occurred %EPON% Epon alarm critical-event occour! sent by NPC 3
Alarm Description	It's a data loading fault or other dying gasp fault. Or fault occurs in receive direction of local data terminal device.
Supported Devices	EPON project of 4822

33291

Message No.	33291
Default Security Level	5
Alarm Type	"CommunicationAlarm"
NM Level	5
Cause	The total number of ONU that connects with OLT in downstream exceeds the specification that system supports.
Influence	EPON device can't run normally for overloading.
Recommended Operations	Limit the number of ONU connections under OLT to 32. This alarm is called onu over limitation alarm in EPON project. In default, this alarm is enabled. If the alarm need to be disabled configure "alarm onu-over-limitation disable" on OLT interface.
Alarm Description Prototype	"Epon alarm onu-over-limitation occour!" Example: 14:57:30 08/26/2008 UTC alarm 33291 occurred %EPON% Epon alarm onu-over-limitation occour! sent by NPC 3
Alarm Description	The number of ONU devices connected to OLT in downstream exceeds 32.
Supported Devices	EPON project of 4822

33292

Message No.	33292
Default Security Level	5
Alarm Type	"CommunicationAlarm"
NM Level	4
Cause	Optical power in upstream that OLT receives from a ONU is too low (lower than OLT sensitivity upper limit) or too high (higher than OLT overload optical power lower limit).
Influence	The optical path is abnormal.
Recommended Operations	Test optical power.
Alarm Description Prototype	"Epon alarm optical-power-overflow occour!" "Epon alarm optical-power-overflow recover!" Example: 10:57:30 08/26/2008 UTC alarm 33292 occurred %EPON% Epon alarm optical-power-overflow occour! sent by NPC 3 Alarm recovery 10:58:10 08/26/2008 UTC alarm 33292 cleared %EPON% Epon alarm optical-power-overflow recover! sent by NPC 3

Alarm Description	Epon optical power overflows.
Supported Devices	EPON project of 4822

33293

Message No.	33293
Default Security Level	5
Alarm Type	"CommunicationAlarm"
NM Level	4
Cause	A ONU gets off-line.
Influence	Alarm occurs.
Alarm Description Prototype	Alarm occur " Epon alarm onu get offline!" Alarm recovery " Epon alarm onu get online!” Example: Alarm occur 9:42:31 08/26/2008 UTC alarm 33293 occurred %EPON% Epon alarm onu get offline! sent by NPC 3 Alarm recovery 9:44:36 08/26/2008 UTC alarm 33293 cleared %EPON% Epon alarm onu get online,onuregister successfully! sent by NPC 3
Alarm Description	ONU gets off-line.
Supported Devices	EPON project of 4822

33294

Message No.	33294
Default Security Level	5
Alarm Type	"CommunicationAlarm"
NM Level	3
Cause	Optical protection switch occurs on EPON.
Influence	Optical protection switch occurs on EPON.
Alarm Description Prototype	"Epon alarm optical protection switch from interface %s to interface %s” The first %sindicate the interface name before switchover. The second %s: indicate the interface name after switchover. Example:

	9:42:31 08/26/2008 UTC alarm 33294 occurred %EPON% Epon alarm optical protection switch from interface epon-olt_3/13 to interface epon-olt_3/14! sent by NPC 3
Alarm Description	Optical protection switch occurs on EPON.
Supported Devices	EPON project of 4822

33295

Message No.	33295
Default Security Level	5
Alarm Type	"QOSAlarm"
NM Level	5
Cause	ONU remote configuration timeouts
Influence	The previous configuration of this ONU is invalid.
Recommended Operations	Please check if the connection between OLT device and ONU device is normal.
Alarm Description Prototype	ONU %s remote configuration timeouts %sOLT sub interface name Example: 00:49:44 12/14/2008 UTC alarm 33295 occurred %EPON% ONU epon-olt_2/16.2 remote configuration timeouts sent by MEC 1
Alarm Description	ONU remote configuration timeouts
Supported Devices	ZXR10 8900

33296

Message No.	33296
Default Security Level	6
Alarm Type	"ProcessingErrorAlarm"
NM Level	5
Cause	ONU remote configuration fails for invalid parameter.
Influence	ONU remote configuration command is invalid.
Recommended Operations	Check if remote configuration ONU command is correct.
Alarm Description Prototype	ONU %s remote configuration fails for invalid parameter %sOLT sub interface name Example: 00:54:34 12/14/2008 UTC alarm 33296 occurred %EPON% ONU epon-olt_2/16.2 remote configuration fails for invalid parameter sent by MEC 1

Alarm Description	ONU remote configuration command is invalid.
Supported Devices	ZXR10 8900

33297

Message No.	33297
Default Security Level	6
Alarm Type	"ProcessingErrorAlarm"
NM Level	5
Cause	ONU remote configuration fails for wrong onu status or capability.
Influence	ONU remote configuration is invalid.
Recommended Operations	Please check if the ONU current status and capability allow to configure this command.
Alarm Description Prototype	ONU %s remote configuration fails for wrong onu status or capability %s OLT sub interface name Example: 00:54:34 12/14/2008 UTC alarm 33296 occurred %EPON% ONU epon-olt_2/16.2 remote configuration fails for wrong onu status or capability
Alarm Description	ONU status is wrong or ONU don't have the capability to configure this command.
Supported Devices	ZXR10 8900

This page is intentionally blank.

Chapter 3

Command Configuration Error Prompt Messages

Table of Contents

Message Format 147
Error Message Description 147

Message Format

Syntax

Error Message Description

10

Message No. 10

Cause The input parameter is illegal.

Recommended Operations Input the correct parameter to try again according to the command prompt and ZXR10 Data Product Command Manual.

11

Message No. 11

Cause Fail to access database.

Recommended Operations Check whether the system operation is normal and the input configuration information is correct. If everything is normal, contact ZTE maintenance staff after recording the error please.

12

Message No. 12

Cause Fail to write to database.

Recommended Operations Check whether the system operation is normal and the configuration is following the normal flow. If everything is correct, contact ZTE maintenance staff after recording the error please.

13

Message No. 13

Cause Fail to send message.

Recommended Operations Check whether the system operation is normal and try again later.

14

Message No. 14

Cause The user does not exist.

Recommended Operations Please input the correct user name for login.

15

Message No. 15

Cause The file does not exist.

Recommended Operations Please input the correct file name.

16

Message No. 16

Cause Incorrect file or directory name.

Recommended Operations Please input the correct file or directory name.

17

Message No. 17

Cause Fail to create timer.

Recommended Operations Check whether the system operation is normal, and try again later if normal.

18

Message No. 18

Cause nvram overflowed

Recommended Operations None.

19

Message No. 19

Cause flash overflowed

Recommended Operations Please delete some useless files in the flash first.

20

Message No. 20

Cause Fail to write nvram.

Recommended Operations Check whether the system operation is normal, and try again later. If unsuccessful, please contact ZTE maintenance staff after recording the error.

21

Message No. 21

Cause Fail to write to flash.

Recommended Operations Check whether the system operation is normal, then, try again when the system is idle.

22

Message No. 22

Cause Fail to read nvram.

Recommended Operations Check whether the system operation is normal and whether nvram is damaged. If everything is normal, try again later please. If the prompt remained, please contact ZTE maintenance staff after recording the error.

23

Message No. 23

Cause Fail to read flash.

Recommended Operations Please check whether the flash exists or being damaged. If everything is normal, please try again later. If fail to retry all the time, please contact ZTE maintenance staff after recording the error.

24

Message No. 24

Cause Fail to write configuration file.

Recommended Operations Check whether the system operation is normal or busy. Please try again when the system is idle. If fail to retry all the time, please contact ZTE maintenance staff after recording the error.

25

Message No. 25

Cause Fail to apply for memory.

Recommended Operations Check whether the system operation is normal, and try again later. If the phenomenon remains, please contact ZTE maintenance staff after recording the error.

26

Message No. 26

Cause Print and Enter.

Recommended Operations None.

27

Message No. 27

Cause Input illegal user name.

Recommended Operations Please input characters accord with the command specification.

28

Message No. 28

Cause Input illegal password.

Recommended Operations Please input characters accord with the command specification.

29

Message No. 29

Cause Input illegal file name.

Recommended Operations Please input characters which can form a file name.

30

Message No. 30

Cause **write** command is executed.

Recommended Operations It may try again later.

31

Message No. 31

Cause Too many directory levels

Recommended Operations Reduce the directory levels.

33

Message No. 33

Cause Boot upgrade is undergoing. Wait please.

Recommended Operations Try again later.

34

Message No. 34

Cause Fail to update boot.

Recommended Operations Please check whether the boot file to upgrade exists. Please stop system traffic and retry when the system is idle. If fail to retry many times, please contact ZTE maintenance staff after recording the error.

35

Message No. 35

Cause The line board to upgrade is offline.

Recommended Operations Please input the correct parameters.

36

Message No. 36

Cause Fail to copy of the boot file to memory.

Recommended Operations Please check whether the file to upgrade boot exists. Please stop system traffic and retry when the system is idle. If fail to retry many times, please contact ZTE maintenance staff after recording the error.

37

Message No. 37

Cause Succeed in bootrom upgrade.

Recommended Operations It is the prompt that system command is executed successfully, no more other operation is needed.

38

Message No. 38

Cause Exchange network is under boot upgrade, wait please.

Recommended Operations The system is carrying out the exchange network boot upgrade; it is suggested that not to perform other operations. Please execute them after system upgrade success.

39

Message No. 39

Cause Fail to upgrade exchange network.

Recommended Operations Fail to upgrade exchange network. Check whether the boot file necessary for exchange network upgrade exists please; If it exists, check whether the system CPU is busy; if busy, try again later. If fail to retry many times, please contact ZTE maintenance staff after recording the error.

40

Message No. 40

Cause The specified board card is offline.

Recommended Operations Check whether the input command is correct please; if correct, check whether the board card with specified slot is operating well; try again after it operates normally. If fail to retry many times, please contact ZTE maintenance staff after recording the error.

41

Message No. 41

Cause Fail to copy file to memory.

Recommended Operations Check whether system CPU is very busy or the specified file exists please. If the file exists, try again later. If fail to retry many times, please contact ZTE maintenance staff after recording the error.

42

Message No. 42

Cause Succeed in exchange network upgrade.

Recommended Operations It is the prompt that command is executed successfully. No more other operations are needed.

44

Message No. 44

Cause There is no response to overtime when writing Img image file.

Recommended Operations Check whether the system is busy, or the system flash exists or is damaged please. If fail to retry many times, please contact ZTE maintenance staff after recording the error.

100

Message No. 100

Cause Fail to send message to ldp process.

Recommended Operations Please check whether the system is running normally and retry when the system is idle.

101

Message No. 101

Cause Fail to extract interface from mpls table.

Recommended Operations Please check whether the input parameter is correct and try again later.

102

Message No. 102

Cause It does not configure enable-mpls command.

Recommended Operations Please execute enable-mpls command first.

103

Message No. 103

Cause The command takes effect at the next start.

Recommended Operations N.A.

104

Message No. 104

Cause router-id cannot be 0.

Recommended Operations Please configure correct command.

105

Message No. 105

Cause Too many ldp interfaces.

Recommended Operations Please configure correct command.

106

Message No. 106

Cause Too many ldp advertise-label controls

Recommended Operations Please configure correct command.

107

Message No. 107

Cause The command takes effect at the next start.

Recommended Operations Reboot the device to take effect.

108

Message No. 108

Cause Too many ldp password settings

Recommended Operations Please configure correct command.

109

Message No. 109

Cause The mpls cannot run at the loopback interface.

Recommended Operations Please configure correct command.

110

Message No. 110

Cause The parameter setting is improper.

Recommended Operations Please set correct command parameter.

112

Message No. 112

Cause The hold time interval of Hello ought to be longer than Hello report interval.

Recommended Operations Check mpls hello hold time interval and hello report interval please; the correct configuration ought to be that hello hold time interval is longer than hello report interval.

201

Message No. 201

Cause The flash is under application.

Recommended Operations Please try again later.

202

Message No. 202

Cause Incorrect copy type

Recommended Operations Please configure correct command.

203

Message No. 203

Cause The (T) FTP server does not respond.

Recommended Operations Check whether the line connection and server operation are normal.

204

Message No. 204

Cause Start to copy.

Recommended Operations Informational notice. No action is needed.

206

Message No. 206

Cause Fail in Network-to-network copy.

Recommended Operations Please input the correct copy command.

207

Message No. 207

Cause The command explanation module sends error messages.

Recommended Operations Please check whether the system is running normally and try again later. If error remained many times, please contact ZTE maintenance staff after recording the error.

208

Message No. 208

Cause Transmit synchronization message incorrectly.

Recommended Operations Please check whether the system is running normally and try again later. If error remained many times, please contact ZTE maintenance staff after recording the error.

209

Message No. 209

Cause Transmit asynchronization message incorrectly.

Recommended Operations Please check whether the system is running normally and try again later. If error remained many times, please contact ZTE maintenance staff after recording the error.

210

Message No. 210

Cause Fail to delete directory.

Recommended Operations Please check whether any file is still under the directory or any user under the current directory. If no, please try again.

211

Message No. 211

Cause Succeed in copying file.

Recommended Operations None.

212

Message No. 212

Cause End the file copy due to errors.

Recommended Operations Check whether the line and system operation are normal. If they are, please try again later.

213

Message No. 213

Cause Fail to transmit the response message.

Recommended Operations Check whether the system running is normal; if normal, please try again later. If error appeared many times, please contact ZTE maintenance staff after recording the error.

214

Message No. 214

Cause It does not support the system file reading and writing temporarily.

Recommended Operations Informational notice. No action is needed.

215

Message No. 215

Cause It does not support the operation.

Recommended Operations Please use the correct command. Refer to the related user manual if possible.

216

Message No. 216

Cause Incorrect file name

Recommended Operations Please configure correct command.

217

Message No. 217

Cause No IP address has been designated.

Recommended Operations Please input the correct address for copy command.

218

Message No. 218

Cause The source file name is the same as target file name during renaming.

Recommended Operations Please input the correct command parameter.

219

Message No. 219

Cause It cannot be changed into the file name.

Recommended Operations Please check whether the input parameter is legal and the command configuration is correct.

220

Message No. 220

Cause It cannot create the directory.

Recommended Operations Please check whether the input parameter is legal and the command configuration is correct.

221

Message No. 221

Cause Fail to delete file.

Recommended Operations Please check whether the input parameter is correct and the file is used.

222

Message No. 222

Cause Fail in dir command operation.

Recommended Operations Please check whether the input parameter is correct and try again later.

223

Message No. 223

Cause FTP server configuration command is wrong.

Recommended Operations Please input the correct parameter and perform correct command configuration.

224

Message No. 224

Cause It succeeds in FTP server configuration command execution.

Recommended Operations Informational notice. No action is needed.

225

Message No. 225

Cause The command execution mode is wrong.

Recommended Operations Please contact ZTE maintenance staff after recording the error.

226

Message No. 226

Cause Incorrect target file name path

Recommended Operations Please input the correct command parameter.

227

Message No. 227

Cause The file name is too long.

Recommended Operations Please input parameters within the range permitted by command.

228

Message No. 228

Cause The source file name is the same as target file name during copying.

Recommended Operations Please input the correct command parameter.

229

Message No. 229

Cause The input date is incorrect.

Recommended Operations Please input the correct command parameter.

230

Message No. 230

Cause It modifies system clock incorrectly.

Recommended Operations Please try again later. If error appeared many times, please contact ZTE maintenance staff after recording the error.

231

Message No. 231

Cause Fail in acl configuration operation.

Recommended Operations Check whether the configuration reaches the maximum system permitted value, and try again later. If fail to retry many times, please contact ZTE maintenance staff after recording the error.

232

Message No. 232

Cause Fail in route-map configuration operation.

Recommended Operations Check whether the configuration command is correct and proper, and try again later. If fail to retry many times, please contact ZTE maintenance staff after recording the error.

233

Message No. 233

Cause Too many parameters entered

Recommended Operations Perform the configuration by following ZXR10 Router/Ethernet Switch Command Manual please.

235

Message No. 235

Cause Input ACL incorrectly.

Recommended Operations Please input the correct command parameter.

236

Message No. 236

Cause The input interface board name is wrong.

Recommended Operations Please input the correct command parameter.

237

Message No. 237

Cause The interface board type is wrong.

Recommended Operations Please check whether the system is running normally and the configuration command parameter is correct.

238

Message No. 238

Cause The ACL number does not exist.

Recommended Operations Please input the correct command parameter.

239

Message No. 239

Cause Fail to set the cos queue classifications.

Recommended Operations Please check whether the input command parameter is correct and proper, and try again later. If fail to retry many times, please contact ZTE maintenance staff after recording the error.

240

Message No. 240

Cause Fail to set the cos IP priority function.

Recommended Operations Please contact ZTE maintenance staff after recording the error. It may try again later.

241

Message No. 241

Cause Fail to set cos IP priority function data.

Recommended Operations Please contact ZTE maintenance staff after recording the error. It may try again later.

242

Message No. 242

Cause This priority does not exist.

Recommended Operations Please check whether the command configuration is proper and the parameter configuration is correct.

243

Message No. 243

Cause The same priority is already existed.

Recommended Operations Informational notice. No action is needed.

244

Message No. 244

Cause Fail in the community-list operation.

Recommended Operations Please check whether the command parameter is correct and proper, and try again later.

245

Message No. 245

Cause The input expression is wrong.

Recommended Operations Please input the correct command.

246

Message No. 246

Cause The ACL rule expression is wrong.

Recommended Operations Please configure correct command.

247

Message No. 247

Cause The source file does not exist.

Recommended Operations Please input the correct command parameter.

248

Message No. 248

Cause The target file name is the same as an existed directory.

Recommended Operations Please input the correct command parameter.

250

Message No. 250

Cause The rule expression is too long.

Recommended Operations Please input the correct command parameter.

251

Message No. 251

Cause Fail to distribute the memory for rule expression.

Recommended Operations Please input the correct command parameter and try again later.

252

Message No. 252

Cause There are too many (,) symbols in the rule expression.

Recommended Operations Please input the correct command parameter.

253

Message No. 253

Cause The () in the rule expression does not pair.

Recommended Operations Please input the correct command parameter.

254

Message No. 254

Cause The () in the rule expression is mismatched.

Recommended Operations Please input the correct command parameter.

255

Message No. 255

Cause Internal error occurs during rule expression generation.

Recommended Operations Please check whether the input command is proper and try again later.

256

Message No. 256

Cause The + and * operations in the rule expression cannot be vacant initially.

Recommended Operations Please input the correct command parameter.

257

Message No. 257

Cause There are too many +*% symbols nested in the rule expression.

Recommended Operations Please input the correct command parameter.

258

Message No. 258

Cause The [,] range in the rule expression is illegal.

Recommended Operations Please input the correct command parameter.

259

Message No. 259

Cause The [,] range in the rule expression is mismatched.

Recommended Operations Please input the correct command parameter.

260

Message No. 260

Cause The content after +, * and % in the rule expression cannot be vacant.

Recommended Operations Please input the correct command parameter.

261

Message No. 261

Cause There are other errors in the rule expression.

Recommended Operations Please input the correct command parameter.

262

Message No. 262

Cause AllView and DefaultView figures cannot be modified or deleted.

Recommended Operations AllView and DefaultView figures are system default figures, which cannot be modified or deleted.

263

Message No. 263

Cause The next hop address is illegal.

Recommended Operations Please input the correct command parameter.

264

Message No. 264

Cause The same ACL item exists.

Recommended Operations Please verify or configure other ACL.

265

Message No. 265

Cause It carries out a special command, wait for a while please.

Recommended Operations Try again later.

266

Message No. 266

Cause The target file is not existed.

Recommended Operations Please input the correct target file.

267

Message No. 267

Cause The copies are wrong, and fail to write file.

Recommended Operations Check whether the system operation is normal, and try again later. If error remained many times, please contact ZTE maintenance staff after recording the error.

268

Message No. 268

Cause Fail in the operation. The target file is under use.

Recommended Operations Please try again later.

269

Message No. 269

Cause The new file name expression is wrong.

Recommended Operations Please input the proper characters according to command parameter requirement.

270

Message No. 270

Cause This command can only be run at the console serial port.

Recommended Operations Please input the correct command.

271

Message No. 271

Cause Fail in the operation. The flash is under use.

Recommended Operations Please try again later.

272

Message No. 272

Cause Fail to access. There are too many users online at present.

Recommended Operations Please try again later.

273

Message No. 273

Cause Fail to access. There are too many users online at present.

Recommended Operations Please try again later.

274

Message No. 274

Cause The physical interface cannot be deleted.

Recommended Operations Input a correct command please.

275

Message No. 275

Cause This command cannot be used at this sub-interface.

Recommended Operations Refer to the related manuals and use this command in the right interface.

276

Message No. 276

Cause This command cannot be used at this interface.

Recommended Operations Refer to the related manuals and use this command in the right interface.

277

Message No. 277

Cause The flash is not existed.

Recommended Operations Please check whether the system is running normally and the flash device exists.

278

Message No. 278

Cause The system provides the reference clock for the interface board.

Recommended Operations None.

279

Message No. 279

Cause This interface does not support a designated clock source.

Recommended Operations None.

280

Message No. 280

Cause This command cannot delete the e1 channelized interface.

Recommended Operations Refer to the related manuals and use this command in the right interface.

284

Message No. 284

Cause The command cannot delete the interface specified in command.

Recommended Operations Check whether the interface parameter in the command configuration is correct and whether the interface attribute can be deleted by this command.

285

Message No. 285

Cause The configured route-map items reach to the limitation.

Recommended Operations Check the configured route-map items and delete some unnecessary items, then perform configuration.

288

Message No. 288

Cause Too many configured prefix-list items, it reaches to permitted item quantity limitation.

Recommended Operations Check the configured prefix-list items and delete some unnecessary items, then perform the configuration.

289

Message No. 289

Cause Fail to write prefix-list to database.

Recommended Operations Check whether the configured prefix-list items reaches to limitation, if not, try again later. If it remains the same after retrying many times, please contact ZTE maintenance staff after recording the error.

290

Message No. 290

Cause Fail to find prefix-list item.

Recommended Operations Check whether the prefix-list in configuration parameter exists.

292

Message No. 292

Cause The input acl alias is used by other acl table number, input other acl alias please.

Recommended Operations Check whether the input acl alias is the one planed to input, or other configuration is incorrect please.

300

Message No. 300

Cause This command cannot be used at this interface.

Recommended Operations None

303

Message No. 303

Cause There is a user accessing the interface configuration mode, and fail to delete the interface.

Recommended Operations It may try again later.

305

Message No. 305

Cause Fail to delete user.

Recommended Operations It may try again later.

306

Message No. 306

Cause Add user incorrectly.

Recommended Operations Please check whether it reaches the maximum configuration. Try again later.

307

Message No. 307

Cause The same user exists.

Recommended Operations None.

308

Message No. 308

Cause The user group does not exist.

Recommended Operations Please perform command configuration in correct sequence and check whether the input parameters are correct.

309

Message No. 309

Cause There is illegal character in user group name.

Recommended Operations Please input the correct parameter.

1001

Message No. 1001

Cause The interface does not exist.

Recommended Operations Please check whether the input parameter is correct.

1002

Message No. 1002

Cause The same network section IP address already exists.

Recommended Operations Please input the correct parameter.

1003

Message No. 1003

Cause Incorrect IP address mask

Recommended Operations Please input the correct parameter.

1004

Message No. 1004

Cause Incorrect IP broadcast address is input.

Recommended Operations Please input the correct parameter.

1005

Message No. 1005

Cause Fail to add IP address.

Recommended Operations Please check whether the parameter is correct and try again later.

1006

Message No. 1006

Cause Fail to delete IP address.

Recommended Operations Please check whether the parameter is correct and try again later.

1007

Message No. 1007

Cause The input IP address does not exist.

Recommended Operations Please input the correct parameter.

1008

Message No. 1008

Cause Fail to add IP address route.

Recommended Operations Please check whether the parameter is correct and try again later.

1009

Message No. 1009

Cause Fail to delete IP address route.

Recommended Operations Please check whether the parameter is correct and try again later.

1010

Message No. 1010

Cause The next hop address is illegal, which cannot be the configured address for router.

Recommended Operations Please input the correct parameter.

1011

Message No. 1011

Cause The next hop address is illegal, which can only be a direct-connect network section address.

Recommended Operations Please input the correct parameter.

1012

Message No. 1012

Cause The memory is insufficient.

Recommended Operations Please remove some configurations not used, and then try again later.

1013

Message No. 1013

Cause There is no idle slot.

Recommended Operations Please check whether it reaches the maximum configuration, and whether it is able to try again later.

1014

Message No. 1014

Cause No route is found.

Recommended Operations Check whether the configuration is correct and whether the connection is normal.

1015

Message No. 1015

Cause The interface is not configured with the route discovery.

Recommended Operations This is the system prompt.

1016

Message No. 1016

Cause The interface has no IP address.

Recommended Operations This is the system prompt.

1017

Message No. 1017

Cause The current unnumber interface has IP address already.

Recommended Operations Please check whether the configuration is proper.

1018

Message No. 1018

Cause Fail in current operation.

Recommended Operations It may try again later.

1019

Message No. 1019

Cause The line board location parameter is wrong.

Recommended Operations Please check whether the command configuration is correct.

1020

Message No. 1020

Cause The board type is wrong.

Recommended Operations Please check whether the input parameter is correct.

1021

Message No. 1021

Cause The interface board already exists.

Recommended Operations This is the system prompt.

1022

Message No. 1022

Cause The interface board does not exist.

Recommended Operations This is the system prompt.

1024

Message No. 1024

Cause The debug of IP packet is activated.

Recommended Operations Informational notice. No action is needed.

1025

Message No. 1025

Cause The debug of IP packet is deactivated.

Recommended Operations Informational notice. No action is needed.

1026

Message No. 1026

Cause The debug of arp packet is activated.

Recommended Operations Informational notice. No action is needed.

1027

Message No. 1027

Cause The debug of arp packet is deactivated.

Recommended Operations Informational notice. No action is needed.

1028

Message No. 1028

Cause The debug of icmp packet is activated.

Recommended Operations Informational notice. No action is needed.

1029

Message No. 1029

Cause The debug of icmp packet is deactivated.

Recommended Operations Informational notice. No action is needed.

1030

Message No. 1030

Cause The host address is illegal.

Recommended Operations Please input the correct parameter.

1031

Message No. 1031

Cause The input address is illegal.

Recommended Operations Please input the correct parameter.

1032

Message No. 1032

Cause This interface is not an Ethernet interface.

Recommended Operations Informational notice. No action is needed.

1033

Message No. 1033

Cause Fail to match the route to delete.

Recommended Operations Please check whether the input parameter is correct.

1034

Message No. 1034

Cause Please remove the ip unnumber attribution of interface first.

Recommended Operations Informational notice. No action is needed.

1035

Message No. 1035

Cause The same tag value exists.

Recommended Operations Please check whether the input parameter is correct.

1036

Message No. 1036

Cause Illegal mtu value

Recommended Operations Please check whether the input parameter value range is legal.

1037

Message No. 1037

Cause The destination address is the local address itself.

Recommended Operations Please configure correct command.

1038

Message No. 1038

Cause The selection packet header length is too short, and illegal.

Recommended Operations Please input the correct parameter and try again later.

1039

Message No. 1039

Cause The address and mask are mismatched.

Recommended Operations Please configure correct command.

1040

Message No. 1040

Cause The option length is incorrect.

Recommended Operations Please configure correct command.

1041

Message No. 1041

Cause illegal source

Recommended Operations Please input the correct command parameter and try again later.

1042

Message No. 1042

Cause The interface has no host address.

Recommended Operations Please input the correct parameter.

1043

Message No. 1043

Cause Auxiliary addresses exist.

Recommended Operations Delete all the auxiliary addresses first.

1044

Message No. 1044

Cause The ip unnumber attribution of interface exists.

Recommended Operations Please remove the ip unnumber attribution of interface first.

1049

Message No. 1049

Cause The input PVC value reaches the maximum limit.

Recommended Operations Please check whether the system configuration is proper and the configuration information reaches the maximum system permitted value.

1050

Message No. 1050

Cause The acl list does not exist.

Recommended Operations Please check whether the parameter acl list is correct and whether the command configuration sequence is proper.

1051

Message No. 1051

Cause Only PVC is allowed on point-to-point network.

Recommended Operations This is the system prompt.

1052

Message No. 1052

Cause PVC does not exist.

Recommended Operations Please check whether the input parameter is correct and the command configuration sequence is proper.

1053

Message No. 1053

Cause Fail to create ATM interface.

Recommended Operations Please check whether the system configuration reaches the maximum value; if not, please try again later.

1054

Message No. 1054

Cause Fail to delete ATM interface.

Recommended Operations Please check whether the input parameter is correct, and try again later.

1055

Message No. 1055

Cause No PVC.

Recommended Operations Please create PVC first.

1056

Message No. 1056

Cause It permits only one IP address to be configured for ATM interface.

Recommended Operations Please configure only one IP address.

1057

Message No. 1057

Cause The point-to-point network permits only one map list.

Recommended Operations Please use only one map list.

1058

Message No. 1058

Cause VCI 1~31 are reserved for ATM, not for PVC creation.

Recommended Operations None.

1059

Message No. 1059

Cause The input vcd already exists.

Recommended Operations Confirm that the input parameter is correct.

1060

Message No. 1060

Cause PVC is used by other interface.

Recommended Operations Please check whether the input parameter is correct and whether the command configuration is proper.

1061

Message No. 1061

Cause This address is conflict with management interface address.

Recommended Operations Please check whether the input parameter is correct and the command configuration is proper.

1062

Message No. 1062

Cause This command cannot run at telnet terminal.

Recommended Operations Refer to the related manuals and input the correct parameters.

1063

Message No. 1063

Cause The input parameter is wrong.

Recommended Operations Please check whether the input parameter is correct.

1064

Message No. 1064

Cause Please unplug/plug the designated interface board.

Recommended Operations Please plug in and plug out the designated interface board.

1070

Message No. 1070

Cause Unable to create the interface

Recommended Operations Please input the correct command parameter.

1071

Message No. 1071

Cause Unable to delete the interface

Recommended Operations Please check whether the command configuration is correct and try again later.

1072

Message No. 1072

Cause The vlan_id is configured already.

Recommended Operations This is the system prompt.

1073

Message No. 1073

Cause There are too many interfaces.

Recommended Operations Please check whether the input parameter is legal and whether the command configuration is proper.

1074

Message No. 1074

Cause There are many interfaces configured on the same board.

Recommended Operations Please check whether the configuration is proper.

1080

Message No. 1080

Cause No arp item exists.

Recommended Operations This is the system prompt.

1081

Message No. 1081

Cause The interface has no arp item.

Recommended Operations This is the system prompt.

1082

Message No. 1082

Cause The designated item does not exist.

Recommended Operations Please check whether the input parameter is correct.

1083

Message No. 1083

Cause The designated item ingress is not bound.

Recommended Operations Please check whether the input parameter is correct.

1500

Message No. 1500

Cause DHCP server is not started.

Recommended Operations Please start DHCP server.

1501

Message No. 1501

Cause DHCP server is not started.

Recommended Operations Please start DHCP server.

1502

Message No. 1502

Cause DHCP relay is still running. Please stop it first.

Recommended Operations Please check whether DHCP server stops working.

1503

Message No. 1503

Cause dhcp relay is started.

Recommended Operations Informational notice. No action is needed.

1504

Message No. 1504

Cause DHCP relay is stopped.

Recommended Operations Check whether DHCP server stops working.

1505

Message No. 1505

Cause DHCP server is started. Please stop it first.

Recommended Operations Please stop DHCP server first.

1700

Message No. 1700

Cause No main RADIUS server, please configure it first.

Recommended Operations please configure main RADIUS server first.

2001

Message No. 2001

Cause No IP example is running.

Recommended Operations None.

2002

Message No. 2002

Cause OSPF example is already running.

Recommended Operations Informational notice. No action is needed.

2003

Message No. 2003

Cause It is not an NBMA interface.

Recommended Operations Please check whether the parameter configuration is correct and proper.

2004

Message No. 2004

Cause No OSPF example is running.

Recommended Operations Please check whether the command configuration sequence is proper and the configuration is correct.

2005

Message No. 2005

Cause The OSPF area does not exist.

Recommended Operations Please check whether the input parameter is correct.

2006

Message No. 2006

Cause The area is disabled.

Recommended Operations Please check whether the command configuration is proper and the parameter is correct.

2007

Message No. 2007

Cause The area is disabled.

Recommended Operations Please check whether the command configuration is proper and whether the parameter is correct.

2008

Message No. 2008

Cause Fail to create OSPF area.

Recommended Operations Please check whether the configuration reaches the maximum system value and try again later.

2009

Message No. 2009

Cause Fail to enable OSPF area.

Recommended Operations It may try again later.

2010

Message No. 2010

Cause Fail to create OSPF example.

Recommended Operations Please check whether the system configuration reaches the maximum limitation, and try again later.

2011

Message No. 2011

Cause Fail to enable OSPF example.

Recommended Operations It may try again later.

2012

Message No. 2012

Cause This area is not NSSA area.

Recommended Operations Please check if the input parameter and the command configuration are correct.

2013

Message No. 2013

Cause Fail to delete the area default information.

Recommended Operations Please check if the command configuration is proper and try again later.

2014

Message No. 2014

Cause Fail to set the area default information.

Recommended Operations Please check if the command configuration is proper and try again later.

2015

Message No. 2015

Cause Fail to delete NSSA area.

Recommended Operations Please check if the command configuration sequence is proper and the command configuration is correct.

2016

Message No. 2016

Cause Fail to change the area to import summary.

Recommended Operations Please check whether the command configuration is proper and correct.

2017

Message No. 2017

Cause Fail to obtain area ingress.

Recommended Operations It may try again later.

2018

Message No. 2018

Cause Fail to delete NSSA area.

Recommended Operations Check whether the command configuration sequence is proper and whether the command configuration is correct.

2019

Message No. 2019

Cause This keyword is not in the interface.

Recommended Operations Check whether the command configuration is correct.

2020

Message No. 2020

Cause A keyword with the same key already exists.

Recommended Operations None.

2021

Message No. 2021

Cause Fail to delete network range.

Recommended Operations It may try again later.

2022

Message No. 2022

Cause Fail to add network range.

Recommended Operations It may try again later.

2023

Message No. 2023

Cause This range is not existed.

Recommended Operations Please check whether the command parameter is correct.

2024

Message No. 2024

Cause OSPF is disabled.

Recommended Operations Please check whether the command configuration sequence is proper and whether the command configuration is correct.

2025

Message No. 2025

Cause The configured authentication type is illegal.

Recommended Operations Please configure correct command.

2026

Message No. 2026

Cause The configured protocol type is illegal.

Recommended Operations Please configure correct command.

2027

Message No. 2027

Cause The virtual interface does not exist.

Recommended Operations Check whether the command configuration parameter is correct and whether the command configuration is proper.

2028

Message No. 2028

Cause The interface name is too long.

Recommended Operations Shorten the interface name.

2029

Message No. 2029

Cause Fail to create OSPF example interface.

Recommended Operations Check whether the command configuration is proper and correct, and try again later.

2030

Message No. 2030

Cause Fail to enable OSPF example interface.

Recommended Operations Check whether the command configuration is correct and try again later.

2031

Message No. 2031

Cause Fail to set area ingress.

Recommended Operations Check whether the command configuration is correct and try again later.

2032

Message No. 2032

Cause Fail to add import filter.

Recommended Operations Check whether the command configuration is correct and try again later.

2033

Message No. 2033

Cause Fail to add export filter.

Recommended Operations Check whether the command configuration is correct and try again later.

2034

Message No. 2034

Cause Fail to delete import filter.

Recommended Operations Check whethewr the command configuration is correct and try again later.

2035

Message No. 2035

Cause The imported template quantity reaches the maximum value.

Recommended Operations None.

2036

Message No. 2036

Cause The exported template quantity reaches the maximum value.

Recommended Operations None.

2037

Message No. 2037

Cause Fail to set area default cost.

Recommended Operations Check whether the command configuration is correct and try again later.

2038

Message No. 2038

Cause Fail to set area virtual connection parameter.

Recommended Operations Check whether the command configuration is correct and try again later.

2039

Message No. 2039

Cause Fail to reset LSA default interval timer.

Recommended Operations It may try again later.

2040

Message No. 2040

Cause Illegal LSA group time slice

Recommended Operations Please check whether the command parameter is correct and whether the parameter configuration is proper.

2041

Message No. 2041

Cause Fail to add the export template.

Recommended Operations It may try again later.

2042

Message No. 2042

Cause Fail to add the import template.

Recommended Operations It may try again later.

2043

Message No. 2043

Cause Fail to delete the export template.

Recommended Operations It may try again later.

2044

Message No. 2044

Cause Fail to delete the import template.

Recommended Operations It may try again later.

2045

Message No. 2045

Cause The address and mask are mismatched.

Recommended Operations Please configure correct command.

2046

Message No. 2046

Cause Unknown protocol type

Recommended Operations Please check if the configuration is correct.

2047

Message No. 2047

Cause The configuration buffer is overflowed.

Recommended Operations Please delete some useless configurations and then try again.

2048

Message No. 2048

Cause The command is incomplete.

Recommended Operations Please configure correct command.

2049

Message No. 2049

Cause Error mask

Recommended Operations Please input the correct command parameter.

2050

Message No. 2050

Cause No backbone area

Recommended Operations Please check whether the command configuration is proper and correct.

2051

Message No. 2051

Cause The backbone area is disabled.

Recommended Operations Please check whether the command configuration is proper.

2052

Message No. 2052

Cause This area is not stub area.

Recommended Operations Please configure correct commands.

2053

Message No. 2053

Cause Unable to obtain router-id.

Recommended Operations Please check whether the command configuration is proper and correct.

2054

Message No. 2054

Cause The stub command is invalid when it is ASBR.

Recommended Operations Please refer to the related manual and input the correct command.

2055

Message No. 2055

Cause This parameter is only used in BGP.

Recommended Operations Please input the correct command.

2056

Message No. 2056

Cause The MD5 keyword configured at the interface reaches the maximum value.

Recommended Operations Decrease or change MD5 keyword.

2057

Message No. 2057

Cause Warning: The router is ASBR but it has only one stub area.

Recommended Operations Check whether the topology is proper.

2058

Message No. 2058

Cause The OSPF neighbor address is a local address.

Recommended Operations Please input the correct configuration parameter.

2059

Message No. 2059

Cause Please input the **clear ip ospf process** command to activate the configuration.

Recommended Operations Execute the command **clear ip ospf process**.

2060

Message No. 2060

Cause The reference bandwidth is changed. Please make sure that the reference bandwidth is consistent in all routers.

Recommended Operations Please confirm the reference bandwidth is consistent in all routers.

2200

Message No. 2200

Cause The vrf command does not match the OSPF example.

Recommended Operations Please check whether the command configuration is correct.

2801

Message No. 2801

Cause The backbone area cannot be configured as an NSSA area.

Recommended Operations This is the system prompt.

2802

Message No. 2802

Cause The stub area cannot be configured as an NSSA area.

Recommended Operations This is the system prompt.

2803

Message No. 2803

Cause The ZXR10 router have only one NSSA area .

Recommended Operations This is the system prompt.

2804

Message No. 2804

Cause It cannot configure NSSA area at stub.

Recommended Operations Please check whether the command configuration is proper.

2805

Message No. 2805

Cause It cannot configure virtual connection across the backbone areas.

Recommended Operations Please check whether the command configuration is proper.

2806

Message No. 2806

Cause It cannot configure virtual connection cross stub or NSSA areas.

Recommended Operations Please check whether the command configuration is correct.

2807

Message No. 2807

Cause The area with virtual connection cannot serve as NSSA area.

Recommended Operations Please configure correct command.

2808

Message No. 2808

Cause The area with a virtual connection cannot serve as stub area.

Recommended Operations Please configure correct command.

2809

Message No. 2809

Cause The backbone area cannot be configured as stub area.

Recommended Operations Please configure correct command.

2810

Message No. 2810

Cause The virtual connection configuration exists in this area.

Recommended Operations Please delete the virtual connection configuration in the area first.

2811

Message No. 2811

Cause The transmission area used by a virtual connection cannot serve as the backbone area.

Recommended Operations Please configure correct command.

2812

Message No. 2812

Cause Please enable the OSPF example first.

Recommended Operations Please enable the OSPF example in global configuration.

2813

Message No. 2813

Cause Virtual connections exists.

Recommended Operations Please delete all virtual connections.

2814

Message No. 2814

Cause The same vrf does not support two examples.

Recommended Operations The same vrf can only choose one example.

2815

Message No. 2815

Cause Please delete all networks in this area first.

Recommended Operations None.

3001

Message No. 3001

Cause No RIP example is running.

Recommended Operations Please check whether the command configuration is proper and correct.

3002

Message No. 3002

Cause No RIP example

Recommended Operations This is the system prompt.

3003

Message No. 3003

Cause It cannot create RIP example.

Recommended Operations Please check whether the system is running normally and try again later.

3004

Message No. 3004

Cause It cannot enable RIP example.

Recommended Operations It may try again later.

3005

Message No. 3005

Cause This keyword does not exist.

Recommended Operations Check whether the command configuration is correct.

3006

Message No. 3006

Cause This neighbor cannot be created.

Recommended Operations Check whether the command configuration is correct and whether the network connection is normal.

3007

Message No. 3007

Cause This neighbor does not exist.

Recommended Operations Please check whether the command configuration is correct.

3008

Message No. 3008

Cause This neighbor cannot be deleted.

Recommended Operations Check whether the command configuration is correct and try again later.

3009

Message No. 3009

Cause The same neighbor already exists on this interface.

Recommended Operations This is the system prompt.

3010

Message No. 3010

Cause Incorrect RIP version

Recommended Operations Please check whether the command configuration is correct and whether it is consistent with the opposite end.

3011

Message No. 3011

Cause No RIP network configuration

Recommended Operations Please check whether the command configuration is proper and correct.

3012

Message No. 3012

Cause Error keyword

Recommended Operations Please configure correct command.

3013

Message No. 3013

Cause The same key id already exists.

Recommended Operations None.

3014

Message No. 3014

Cause Errors redistribution

Recommended Operations Check whether the system running is normal and whether the command configuration is correct and proper.

3015

Message No. 3015

Cause The network does not exist.

Recommended Operations Please check whether the command configuration is correct.

3016

Message No. 3016

Cause Error D or E type network

Recommended Operations Please configure correct command.

3017

Message No. 3017

Cause Loopback network error

Recommended Operations Please configure correct command.

3018

Message No. 3018

Cause Error, the mask is discontinuous.

Recommended Operations Please configure correct command.

4001

Message No. 4001

Cause It is only the A, B or C type network.

Recommended Operations This is the system prompt.

4002

Message No. 4002

Cause The network mask is discontinuous.

Recommended Operations Please configure correct command.

4003

Message No. 4003

Cause The network does not match the mask.

Recommended Operations Please configure correct command.

4004

Message No. 4004

Cause The subnet must match the subnet mask.

Recommended Operations Please configure correct command.

4005

Message No. 4005

Cause The subnet mask must match the subnet.

Recommended Operations Please configure correct command.

4006

Message No. 4006

Cause The network parameters must contain the mask.

Recommended Operations Please configure correct command.

4007

Message No. 4007

Cause The mask parameter must be at the network side.

Recommended Operations Please configure correct command.

4008

Message No. 4008

Cause The mask is too short.

Recommended Operations Please configure correct command.

4009

Message No. 4009

Cause This subnet is not a subnet of the designated network.

Recommended Operations Please configure correct command.

4010

Message No. 4010

Cause Illegal neighbor address

Recommended Operations Please input the correct command configuration parameter.

4011

Message No. 4011

Cause Illegal protocol name

Recommended Operations Please input the correct command parameter.

4012

Message No. 4012

Cause holdtime must be 0 or 3~65535.

Recommended Operations Please input the correct command configuration parameter.

4013

Message No. 4013

Cause The input value is mismatched. Please adjust or use the default value.

Recommended Operations Please input the correct command parameter.

4014

Message No. 4014

Cause The suppression value must be more than the reuse value.

Recommended Operations Please configure correct command.

4015

Message No. 4015

Cause The maximum cycle of the suppression value must be over one half of the life cycle.

Recommended Operations Please input the correct configuration parameter.

4016

Message No. 4016

Cause 0 as a mask is illegal.

Recommended Operations Please input the correct command parameter.

4030

Message No. 4030

Cause The BGP module is not existed.

Recommended Operations Please check if the system is running correctly and the command configuration is proper.

4031

Message No. 4031

Cause This neighbor does not exist.

Recommended Operations Please check whether the command configuration parameter is correct.

4032

Message No. 4032

Cause This neighbor already exists.

Recommended Operations This is the system prompt.

4033

Message No. 4033

Cause There is no aggregation policy.

Recommended Operations Please set the aggregation policy first.

4034

Message No. 4034

Cause The interface does not exist.

Recommended Operations Please check whether the input parameter is correct.

4035

Message No. 4035

Cause This policy does not exist or cannot be deleted.

Recommended Operations Please check whether the input parameter is correct, and try again later.

4036

Message No. 4036

Cause It supports maximum 3 neighbors' debug function at one time.

Recommended Operations This is the system prompt.

4037

Message No. 4037

Cause The neighbor's update debug function is not enabled.

Recommended Operations This is the system prompt.

4038

Message No. 4038

Cause Reflect can be configured only at the internal end point.

Recommended Operations This is the system prompt.

4039

Message No. 4039

Cause It cannot configure local system as a neighbor.

Recommended Operations Please check whether the command configuration is correct.

4040

Message No. 4040

Cause It cannot delete private AS from IBGP end point.

Recommended Operations Please check whether the command configuration is proper and correct.

4041

Message No. 4041

Cause The neighbor is configured as RR-client. Please delete the attribution first.

Recommended Operations Check whether the command configuration sequence is proper and the command configuration is correct.

4042

Message No. 4042

Cause The coalition end point quantity exceeds the maximum value.

Recommended Operations This is the system prompt.

4043

Message No. 4043

Cause The command is run in common user mode.

Recommended Operations Please configure correct command.

4044

Message No. 4044

Cause The coalition interface inputs cannot exceed 50.

Recommended Operations This is the system prompt.

4045

Message No. 4045

Cause Alliance interface is configured. Please remove it first.

Recommended Operations Please remove alliance interface.

4046

Message No. 4046

Cause Please configure the coalition ID first.

Recommended Operations Please check whether the command configuration sequence is proper and whether the command configuration is correct.

4047

Message No. 4047

Cause No local AS member is allowed existing in coalition node list.

Recommended Operations Please check whether the command configuration is proper.

4048

Message No. 4048

Cause No address-family example

Recommended Operations Please check whether the command configuration is correct.

4049

Message No. 4049

Cause cluster id number cannot be 0.

Recommended Operations Please input correct command parameter and perform correct command configuration.

4501

Message No. 4501

Cause No ISIS example is running.

Recommended Operations Please check whether the configuration is correct.

4502

Message No. 4502

Cause The area address quantity reaches the maximum value.

Recommended Operations This is the system prompt.

4503

Message No. 4503

Cause No priority can be set in ppp connection.

Recommended Operations Please check whether the command configuration is correct.

4504

Message No. 4504

Cause No DIS parameter can be set at a non-broadcast interface.

Recommended Operations This is the system prompt.

4505

Message No. 4505

Cause No retransmission interval can be set at a broadcast interface.

Recommended Operations Please check whether the command configuration is correct.

4506

Message No. 4506

Cause The no router isis command is executed. Please try again later.

Recommended Operations Try again later.

4507

Message No. 4507

Cause The isis route is being deleted since the level varies. Please try again later.

Recommended Operations Try again later.

4508

Message No. 4508

Cause system-id exceeds the permitted range.

Recommended Operations Please check whether the input parameter is correct and proper.

4509

Message No. 4509

Cause It is not allowed to change the system-id when changing the system-id range.

Recommended Operations Please do not change the system-id.

4510

Message No. 4510

Cause It is not allowed to modify the system id when a system id exists already.

Recommended Operations Please do not change the system-id.

4511

Message No. 4511

Cause The external metric type cannot be set as always default notify route.

Recommended Operations Please check whether the input parameter is correct.

4512

Message No. 4512

Cause The narrow sense metric type range is 0~63.

Recommended Operations Please check whether the input command parameter is correct.

5001

Message No. 5001

Cause The TCP connection does not exist.

Recommended Operations Please check whether the input command parameter is correct.

5002

Message No. 5002

Cause The TCP connection used by BGP cannot be cleared.

Recommended Operations This is the system prompt.

5003

Message No. 5003

Cause The TCP connection is not set up.

Recommended Operations Please check whether the configuration is correct and whether ACL blocks the TCP connection.

5004

Message No. 5004

Cause Fail in connection and shut down the telnet.

Recommended Operations Please try again later.

5005

Message No. 5005

Cause The memory cannot be distributed and there is no way to start TCP connection.

Recommended Operations Please try again later.

5006

Message No. 5006

Cause TCP connection does not exist or cannot be cleared.

Recommended Operations Please try again later.

5007

Message No. 5007

Cause The ip vrf routing table does not exist.

Recommended Operations Please check if the command configuration and parameter are correct.

6001

Message No. 6001

Cause Error RMON group number

Recommended Operations Please confirm whether the current version supports RMON-related groups and the command configuration is correct.

6010

Message No. 6010

Cause Error data in received message packet

Recommended Operations Please try again later.

6011

Message No. 6011

Cause Error header of received packet

Recommended Operations Please try again later.

6012

Message No. 6012

Cause The received internal message return area is blank.

Recommended Operations Please try again later.

6020

Message No. 6020

Cause Error ID of received message

Recommended Operations Please check whether the command and command parameters are correct.

6021

Message No. 6021

Cause Error command ID of received command message

Recommended Operations Please check whether RMON supports the command and whether the command configuration is correct.

6022

Message No. 6022

Cause Error command parameter

Recommended Operations Please check whether the input command parameter is valid and proper.

6023

Message No. 6023

Cause The received command parameter quantity is wrong.

Recommended Operations Please check whether the input parameter is correct.

6024

Message No. 6024

Cause The index is wrong.

Recommended Operations Please check whether the command parameter and command configuration are correct.

6025

Message No. 6025

Cause Fail to distribute buffer.

Recommended Operations Please check whether the RMON configuration reaches the maximum system value and try again later.

6026

Message No. 6026

Cause Module conflict

Recommended Operations Please check if the command configuration is correct and try again later.

6027

Message No. 6027

Cause Error ingress deletion (index not existed or mismatched)

Recommended Operations Please check if the command parameter is correct.

6028

Message No. 6028

Cause Fail to add ingress.

Recommended Operations Please check if the parameter is correct and try again later.

6029

Message No. 6029

Cause No RMON-related information

Recommended Operations This is the system prompt.

6030

Message No. 6030

Cause The statistics table is blank.

Recommended Operations This is the system prompt.

6031

Message No. 6031

Cause The history table is blank.

Recommended Operations This is the system prompt.

6032

Message No. 6032

Cause The history table is blank.

Recommended Operations This is the system prompt.

6033

Message No. 6033

Cause The host table is blank.

Recommended Operations This is the system prompt.

6034

Message No. 6034

Cause The highest N host tables are blank.

Recommended Operations This is the system prompt.

6035

Message No. 6035

Cause The matrix table is blank.

Recommended Operations This is the system prompt.

6036

Message No. 6036

Cause The filter table is blank.

Recommended Operations This is the system prompt.

6037

Message No. 6037

Cause The capture table is blank.

Recommended Operations This is the system prompt.

6038

Message No. 6038

Cause The event table is blank.

Recommended Operations This is the system prompt.

6040

Message No. 6040

Cause The RMON timer is wrong.

Recommended Operations Please try again later.

6050

Message No. 6050

Cause The start function failure

Recommended Operations Please try again later.

6051

Message No. 6051

Cause No interface information

Recommended Operations Please check whether the system is running normally and whether the parameter is correct.

6052

Message No. 6052

Cause The packet received from the line card is wrong.

Recommended Operations Please check whether the system is running normally and whether the parameter is correct.

6053

Message No. 6053

Cause The sampling type is wrong.

Recommended Operations Please check whether the command configuration is correct and try again later.

6054

Message No. 6054

Cause Incorrect OID

Recommended Operations Please input the correct parameter and try again later.

6055

Message No. 6055

Cause Add event table incorrectly.

Recommended Operations Please try again later.

6056

Message No. 6056

Cause Add channel ingress incorrectly.

Recommended Operations Please try again later.

6057

Message No. 6057

Cause The resources do not exist.

Recommended Operations Please check whether the system is running normally; whether the input parameter is correct; and whether the equipment to monitor is running normally.

6058

Message No. 6058

Cause The function is enabled.

Recommended Operations This is the system prompt.

6059

Message No. 6059

Cause The index exists already.

Recommended Operations This is the system prompt.

6080

Message No. 6080

Cause Ethernet statistics index number error

Recommended Operations Please configure correct command.

6081

Message No. 6081

Cause Ethernet history control index number error

Recommended Operations Please configure correct command.

6082

Message No. 6082

Cause Alarm index number error

Recommended Operations Please configure correct command.

6083

Message No. 6083

Cause Host control table index number error

Recommended Operations Please configure correct command.

6084

Message No. 6084

Cause The highest **N** host table index number errors

Recommended Operations Please configure correct command.

6085

Message No. 6085

Cause Matrix control table index number error

Recommended Operations Please configure correct command.

6086

Message No. 6086

Cause Filter table index number error

Recommended Operations Please configure correct command.

6087

Message No. 6087

Cause Channel table index number error

Recommended Operations Please configure correct command.

6088

Message No. 6088

Cause Buffer control table index number error

Recommended Operations None.

6089

Message No. 6089

Cause Event table index number error

Recommended Operations Please configure correct command.

6601

Message No. 6601

Cause NTP cannot identify the server.

Recommended Operations Please check whether the configuration parameter is correct.

7001

Message No. 7001

Cause Message ID error

Recommended Operations This is the system prompt.

7002

Message No. 7002

Cause Incorrect pointer to obtain synchronous message return

Recommended Operations Please try again later.

7003

Message No. 7003

Cause Too short synchronous message return area length

Recommended Operations Please try again later.

7004

Message No. 7004

Cause Error asynchronization message

Recommended Operations Please try again later.

7005

Message No. 7005

Cause No data in synchronous message

Recommended Operations Please try again later.

7006

Message No. 7006

Cause Error message data header

Recommended Operations This is the system prompt. Please try again later.

7007

Message No. 7007

Cause Error process status

Recommended Operations Please check whether the system is running normally.

7008

Message No. 7008

Cause Fail in initialization.

Recommended Operations Please check whether the system is running normally.

7010

Message No. 7010

Cause Memory application failure

Recommended Operations Please check whether the system is running normally.

7011

Message No. 7011

Cause Memory release failure

Recommended Operations Please try again later.

7012

Message No. 7012

Cause Error internal communication status

Recommended Operations Please try again later.

7020

Message No. 7020

Cause Fail to write to database.

Recommended Operations Please try again later.

7021

Message No. 7021

Cause Fail to access database.

Recommended Operations Please try again later.

7022

Message No. 7022

Cause Fail to delete database.

Recommended Operations Please try again later.

7023

Message No. 7023

Cause Incorrect database path location

Recommended Operations Please try again later.

7024

Message No. 7024

Cause The database process is busy. Please try again later.

Recommended Operations Please try again later.

7030

Message No. 7030

Cause Incorrect command parameter quantity

Recommended Operations Please input the correct command parameter.

7031

Message No. 7031

Cause Error command parameter

Recommended Operations Please check if the input parameter is correct.

7032

Message No. 7032

Cause Error command message ID

Recommended Operations Please check whether the system supports this command.

7040

Message No. 7040

Cause The main log switch is turned off.

Recommended Operations Please turn on the main log switch first.

7041

Message No. 7041

Cause FTP host address is blank.

Recommended Operations Please configure correct command.

7042

Message No. 7042

Cause trap host address is blank.

Recommended Operations Please configure correct command.

7050

Message No. 7050

Cause Error timer ID

Recommended Operations Please check whether the system is running normally.

7051

Message No. 7051

Cause Timer error occurs when starting log file timing.

Recommended Operations Please try again later.

7052

Message No. 7052

Cause Timer error occurs when starting log timing saving.

Recommended Operations Please try again later.

7053

Message No. 7053

Cause Error pointers to obtain the message return area

Recommended Operations Please try again later.

7061

Message No. 7061

Cause Error alarm ID

Recommended Operations Please check whether the input parameter is correct.

7062

Message No. 7062

Cause Error level corresponding to alarm ID

Recommended Operations Please check whether the input parameter is correct.

7063

Message No. 7063

Cause Error alarm type

Recommended Operations Please check whether the input parameter is correct.

7064

Message No. 7064

Cause Error occurs when searching alarm operations.

Recommended Operations Please try again later.

7065

Message No. 7065

Cause The alarm level corresponding to the alarm ID cannot be changed as the specific value.

Recommended Operations Please check whether the input parameter is correct.

7066

Message No. 7066

Cause The alarm level corresponding to the alarm ID cannot be changed.

Recommended Operations Please check whether the input parameter is correct.

7067

Message No. 7067

Cause Fail to write alarm log file.

Recommended Operations Please try again later.

7068

Message No. 7068

Cause Write alarm log file successfully.

Recommended Operations Informational notice. No action is needed.

7069

Message No. 7069

Cause Fail to clear the content in the alarm buffer.

Recommended Operations Please try again later.

7071

Message No. 7071

Cause Fail to set the unified NM trap host address.

Recommended Operations Please try again later.

7081

Message No. 7081

Cause Error board type

Recommended Operations Please check whether the input parameter is correct.

7082

Message No. 7082

Cause Error port ID

Recommended Operations Please input the correct parameter.

7083

Message No. 7083

Cause Error occurs when converting the panel ID to the unit ID.

Recommended Operations Please try again later.

7091

Message No. 7091

Cause syslog server configuring quantity reaches the maximum value.

Recommended Operations Delete the redundant syslog server.

8008

Message No. 8008

Cause SNMP V1 does not support the message.

Recommended Operations Please configure correct command.

8009

Message No. 8009

Cause The buffer is insufficient.

Recommended Operations Please try again later.

8010

Message No. 8010

Cause Error occurs when obtaining configuration information.

Recommended Operations Please try again later.

8011

Message No. 8011

Cause Error occurs when creating encrypted key.

Recommended Operations Please try again later.

8501

Message No. 8501

Cause Error authentication protocol type

Recommended Operations Please check whether the command configuration is correct.

8502

Message No. 8502

Cause The host name is too long.

Recommended Operations Please check whether the input parameter is proper.

8503

Message No. 8503

Cause The password character string is too long.

Recommended Operations Please check whether the input parameter is proper.

8504

Message No. 8504

Cause Error board type

Recommended Operations Please check whether the input parameter is correct.

8505

Message No. 8505

Cause PPP is not configured on this interface.

Recommended Operations Please check whether the system configuration is correct.

8506

Message No. 8506

Cause No PPP example on this interface

Recommended Operations Please check whether the system configuration is correct.

8509

Message No. 8509

Cause This interface does not support PPP.

Recommended Operations Please check whether the command configuration is correct.

8510

Message No. 8510

Cause The pool name does not exist.

Recommended Operations Please check whether the command configuration is correct.

8511

Message No. 8511

Cause Error IP address range

Recommended Operations Please check whether the input parameter is correct.

8512

Message No. 8512

Cause There is no available memory.

Recommended Operations Please check whether the configuration reaches the system permitted maximum value, and try again later after removing some useless configurations.

8513

Message No. 8513

Cause The IP address range of address pool is overlapped.

Recommended Operations There can't be repeated addresses in address pool. Please reset it.

8514

Message No. 8514

Cause The IP address pool does not allow the IP address.

Recommended Operations Please check whether the input parameter is correct.

8515

Message No. 8515

Cause The address is used at interface.

Recommended Operations Please check whether the system configuration is proper.

8516

Message No. 8516

Cause The subscriber is online.

Recommended Operations This is the system prompt.

8517

Message No. 8517

Cause Please check the encryption type.

Recommended Operations Please check whether the command configuration is correct.

8601

Message No. 8601

Cause Fail to add address pool.

Recommended Operations Please try again later.

8602

Message No. 8602

Cause Fail to delete address pool.

Recommended Operations Please try again later.

8603

Message No. 8603

Cause Fail to add rules.

Recommended Operations Please check whether the command configuration is correct and reaches the maximum system permitted value, and then try again later.

8604

Message No. 8604

Cause Fail to delete rules.

Recommended Operations Please try again later.

8605

Message No. 8605

Cause Fail in interface configuration.

Recommended Operations Please try again later.

8606

Message No. 8606

Cause Fail in interface configuration.

Recommended Operations Please try again later.

8607

Message No. 8607

Cause NAT board is not got ready.

Recommended Operations Please try again later.

8608

Message No. 8608

Cause Fail to stop NAT board.

Recommended Operations Please try again later.

8609

Message No. 8609

Cause NAT board is started.

Recommended Operations This is the system prompt.

8610

Message No. 8610

Cause Addresses in this address pool are under application.

Recommended Operations Please try again later.

8611

Message No. 8611

Cause The end address is smaller than the start address.

Recommended Operations Please check whether the input parameter is correct.

8612

Message No. 8612

Cause The address prefix is too long.

Recommended Operations Please check whether the input parameter range is proper.

8613

Message No. 8613

Cause This interface is not configured as inside interface.

Recommended Operations Please check whether the command configuration is correct.

8614

Message No. 8614

Cause This interface is not set as outside interface.

Recommended Operations Please check whether the command configuration is correct.

8615

Message No. 8615

Cause The designated rule does not exist.

Recommended Operations Please check whether the input parameter is correct.

8616

Message No. 8616

Cause The designated address pool does not exist.

Recommended Operations Please check whether the input parameter is correct.

8617

Message No. 8617

Cause The host bit cannot be full 0 or full 1.

Recommended Operations Please check whether the command parameter is correct.

8618

Message No. 8618

Cause The address pool name or address conflicts with others.

Recommended Operations Please check whether the command configuration is proper and correct.

8619

Message No. 8619

Cause The rule and other rule employ the same address pool or acl rule.

Recommended Operations Please check whether the command configuration is correct.

8620

Message No. 8620

Cause The static rule already exists.

Recommended Operations This is the system prompt.

8621

Message No. 8621

Cause It exceeds the maximum permitted quantity of address pools or rules.

Recommended Operations This is the system prompt. Please confirm that there is no conflict between the rules and the application.

8622

Message No. 8622

Cause Some addresses in address pool are used by other address pool.

Recommended Operations Please configure correct command.

8623

Message No. 8623

Cause Address confliction exists in the address pool and static rule.

Recommended Operations Please configure correct command.

8624

Message No. 8624

Cause Address confliction exists in the static rule and dynamic rule.

Recommended Operations Please configure correct command.

8625

Message No. 8625

Cause Please encapsulate VLAN-ID at the interface first.

Recommended Operations This is the system prompt.

8626

Message No. 8626

Cause Fail to delete interface attribution.

Recommended Operations Please try again later.

8701

Message No. 8701

Cause Fail to create E1 interface.

Recommended Operations Please check whether the command configuration is proper and try again later.

8702

Message No. 8702

Cause This channelized group does not exist.

Recommended Operations Please check whether the command configuration is correct.

8703

Message No. 8703

Cause The time slot is used by another channel.

Recommended Operations Please check whether the parameter configuration is correct.

8704

Message No. 8704

Cause Too many channels are configured.

Recommended Operations Please check whether the system configuration is proper.

8705

Message No. 8705

Cause Please modify the frame encapsulation form of E1 interface first.

Recommended Operations This is the system prompt.

8706

Message No. 8706

Cause Please exit the diagnosis mode first.

Recommended Operations Please exit the diagnosis mode and then input the command.

8707

Message No. 8707

Cause Please exit the multi-linkset configuration mode first.

Recommended Operations Please exit the multi-linkset configuration mode and then input the command.

8708

Message No. 8708

Cause The command is illegal.

Recommended Operations Please check whether the command is supported in the mode.

8801

Message No. 8801

Cause vrf does not exist.

Recommended Operations Please check whether the command configuration is correct.

8802

Message No. 8802

Cause The command **no ip vrf** is not executed.

Recommended Operations Please run **no ip vrf** command before configuring vrf.

8803

Message No. 8803

Cause RD cannot be set. Please confirm the value is unique.

Recommended Operations Please confirm RD value is unique.

8804

Message No. 8804

Cause VRF is being deleted.

Recommended Operations Please try again later.

8805

Message No. 8805

Cause VRF has no RD or is being deleted.

Recommended Operations Please try again later.

8806

Message No. 8806

Cause VRF does not exist, or it has no RD.

Recommended Operations Please check whether the command configuration is correct.

8901

Message No. 8901

Cause No frame-relay example at the interface

Recommended Operations Please check whether the command configuration is correct.

8903

Message No. 8903

Cause The address already exists in the map .

Recommended Operations Please check whether the input parameter is correct and proper.

8904

Message No. 8904

Cause The system has no available memory.

Recommended Operations Please try again after removing some useless configurations.

8905

Message No. 8905

Cause No address map can be found for the IP.

Recommended Operations Check whether the related configuration is correct.

8906

Message No. 8906

Cause No frame-relay is configured.

Recommended Operations Please check whether the system configuration is correct.

8907

Message No. 8907

Cause Error frame-relay parameter

Recommended Operations Please check whether the input parameter is correct.

8908

Message No. 8908

Cause To configure DCE/NNI must enable frame-relay exchange.

Recommended Operations Please check whether the command configuration sequence is proper and the command configuration is correct.

8909

Message No. 8909

Cause The command frame-relay encapsulation is not run.

Recommended Operations Please run frame-relay encapsulation command first.

8910

Message No. 8910

Cause The interface does not support frame-relay.

Recommended Operations This is the system prompt.

8911

Message No. 8911

Cause frame-relay LMI debug is closed.

Recommended Operations This is the system prompt.

8912

Message No. 8912

Cause The frame-relay packet debug is closed.

Recommended Operations This is the system prompt.

8913

Message No. 8913

Cause The frame-relay LMI debug is opened.

Recommended Operations This is the system prompt.

8914

Message No. 8914

Cause The frame-relay packet debug is opened.

Recommended Operations This is the system prompt.

8915

Message No. 8915

Cause It cannot ser DTE value for FR DCE.

Recommended Operations Please check whether the command configuration is correct.

8916

Message No. 8916

Cause It cannot set DCE/NNI value for FR DTE.

Recommended Operations Please check whether the command configuration is correct.

8917

Message No. 8917

Cause The frame-relay keep-alive interval cannot exceed 30s. The value will be set as 29s.

Recommended Operations This is the system prompt.

8918

Message No. 8918

Cause No frame-relay is configured for the interface.

Recommended Operations Please check whether the command configuration is proper and correct.

8919

Message No. 8919

Cause The interface PVC quantity reaches the upper limit, unable to create PVC any more.

Recommended Operations This is the system prompt.

8951

Message No. 8951

Cause Fail to create multi-link.

Recommended Operations Please try again later.

8952

Message No. 8952

Cause Fail to find main connection.

Recommended Operations Please check whether the command configuration is correct.

8953

Message No. 8953

Cause Fail to bind on different line boards.

Recommended Operations Please check whether the command configuration is proper and correct.

8954

Message No. 8954

Cause There are too many members at buddle.

Recommended Operations Please check whether the command configuration is correct.

8955

Message No. 8955

Cause Fail to find main connection.

Recommended Operations Please check whether the command configuration is proper and correct.

8956

Message No. 8956

Cause No member interface

Recommended Operations Please check whether the command configuration is correct.

9001

Message No. 9001

Cause The interface is not existed.

Recommended Operations Please check whether the input command parameter is correct.

9002

Message No. 9002

Cause No address is configured on this interface.

Recommended Operations Please check whether the command configuration is proper.

9003

Message No. 9003

Cause Operation failure.

Recommended Operations Please try again later.

9004

Message No. 9004

Cause The acl table ID does not exist.

Recommended Operations Please check whether the command parameter is correct.

9005

Message No. 9005

Cause The group broadcast routing table does not exist.

Recommended Operations Please check whether the system is running correctly and the configuration is correct.

9101

Message No. 9101

Cause The pimdm is started on this interface.

Recommended Operations This is the system prompt.

9102

Message No. 9102

Cause The pimdm is not started on this interface.

Recommended Operations None.

9103

Message No. 9103

Cause The pimdm has no matched group broadcast routing table ingress.

Recommended Operations Please check whether the system command configuration is correct and proper.

9105

Message No. 9105

Cause The interface is disabled.

Recommended Operations This is the system prompt. Check whether the shutdown of this interface influences other protocols or procesure.

9106

Message No. 9106

Cause The pim spare mode is configured.

Recommended Operations This is the system prompt.

9201

Message No. 9201

Cause The pimsm is running on this interface.

Recommended Operations This is the system prompt.

9202

Message No. 9202

Cause The pimsm is not started on this interface.

Recommended Operations This is the system prompt.

9203

Message No. 9203

Cause The spt threshold does not exist.

Recommended Operations Please check whether the command configuration is proper and correct.

9204

Message No. 9204

Cause The pim dense mode is configured.

Recommended Operations This is the system prompt.

9501

Message No. 9501

Cause There are few interfaces in the channel group.

Recommended Operations Please check whether the system configuration is correct and proper.

9502

Message No. 9502

Cause Error parameter type

Recommended Operations Please check whether the command parameter is correct.

9503

Message No. 9503

Cause The group ID range is 1~64.

Recommended Operations This is the system prompt.

9506

Message No. 9506

Cause The group ID is used by another interface.

Recommended Operations Please check whether the input parameter is correct and proper.

9507

Message No. 9507

Cause Error interface configuration mode

Recommended Operations Please check whether the command configuration is proper and correct.

9508

Message No. 9508

Cause This group does not exist.

Recommended Operations Please check whether the command parameter is correct.

9510

Message No. 9510

Cause The system memory is insufficient.

Recommended Operations Please try again after deleting some useless configurations of the system.

9511

Message No. 9511

Cause Some interfaces in the group do not exist.

Recommended Operations Please check whether the system configuration is proper and the input parameter is correct.

9512

Message No. 9512

Cause There are too many group members.

Recommended Operations Please check whether the system configuration is proper.

9513

Message No. 9513

Cause Fail to configure the port auto mode.

Recommended Operations Please try again later.

9514

Message No. 9514

Cause No group.

Recommended Operations Please check whether the command parameter is correct.

9515

Message No. 9515

Cause Error input channel mode

Recommended Operations Please check whether the command parameter is correct.

9516

Message No. 9516

Cause Please allocate the above interfaces to the same management group first.

Recommended Operations Please check whether the system configuration is correct and proper.

9517

Message No. 9517

Cause Repeated interfaces exist in the management group.

Recommended Operations Please check whether the system configuration is correct and proper.

9518

Message No. 9518

Cause No interface in the group

Recommended Operations Please check whether the system configuration is correct and proper.

9519

Message No. 9519

Cause Too many interfaces (the interface quantity should be less than or equal to 16).

Recommended Operations Please check whether the command parameter is correct.

9520

Message No. 9520

Cause Please allocate the above interfaces to the same vlan first.

Recommended Operations Please check whether the system configuration is proper and correct.

9521

Message No. 9521

Cause The buffer reserved for show command is overflowed.

Recommended Operations Please try again after deleting some useless configurations.

9522

Message No. 9522

Cause Lacp can be configured for Ethernet interface type only.

Recommended Operations Please check whether the command configuration is proper and correct.

9523

Message No. 9523

Cause The interface does not support LACP.

Recommended Operations Please check whether the command configuration is proper and correct.

9601

Message No. 9601

Cause Error operation

Recommended Operations Please try again later.

9602

Message No. 9602

Cause The IP address already exists in interface address group.

Recommended Operations Please check whether the command parameter is correct.

9603

Message No. 9603

Cause IP address conflicts with the one at other interface.

Recommended Operations Please check whether the command parameter is correct.

9604

Message No. 9604

Cause Illegal IP address

Recommended Operations Please check whether the command parameter is correct.

9605

Message No. 9605

Cause The ingress does not exist.

Recommended Operations Please check whether the command configuration is correct.

9606

Message No. 9606

Cause No group

Recommended Operations Please check whether the command configuration is correct.

9607

Message No. 9607

Cause The addresses quantity exceeds 100.

Recommended Operations Please check whether the command parameter is correct and proper.

12401

Message Number 12401

Alarm Reason The number of Template exceeds the maximum value.

Recommended Operations Delete some unused Template.

12402

Message Number 12402

Alarm Reason Nat ip is configured in Template of the fire wall which will be deleted.

Recommended Operations Delete Nat ip which is configured in Template of fire wall.

12403

Message Number 12403

Alarm Reason This Template doesn't exist.

Recommended Operations Create Template first.

12404

Message Number 12404

Alarm Reason The interface board is not a firewall interface board.

Recommended Operations Verify the type of the interface board.

12405

Message Number 12405

Alarm Reason The configured Nat ip exceeds the maximum value.

Recommended Operations Don't configure more Nat ip or delete some useless Nat ip.

12406

Message Number 12406

Alarm Reason This Template doesn't bind FW board or DPI board.

Recommended Operations Bind FW board or DPI board first.

12407

Message Number 12407

Alarm Reason This Template has been bound with other Vlan.

Recommended Operations Release the Template binding with other Vlan.

12409

Message Number 12409

Alarm Reason This Nat ip doesn't exist in this Template.

Recommended Operations Verify whether this Nat ip is configured.

12410

Message Number 12410

Alarm Reason This Vlan interface has been bound in a Template.

Recommended Operations Verify which Template this interface has been bound in.

12411

Message Number 12411

Alarm Reason This VLan interface binds with management IP.

Recommended Operations Verify whether this management ip is configured.

12420

Message Number 12420

Alarm Reason This signature entry doesn't exist.

Recommended Operations Create this signature entry first.

12421

Message Number 12421

Alarm Reason This signature symbol doesn't exist.

Recommended Operations Create this signature symbol first.

12422

Message Number 12422

Alarm Reason This flow pool doesn't exist.

Recommended Operations Create this flow pool first.

12423

Message Number 12423

Alarm Reason This service doesn't exist.

Recommended Operations Create this service first.

12424

Message Number 12424

Alarm Reason This subservice doesn't exist.

Recommended Operations Create this subservice first.

12425

Message Number 12425

Alarm Reason The interface board is not a DPI board.

Recommended Operations Verify the type of the interface board.

12426

Message Number 12426

Alarm Reason This Vlan interface has been bound with a DPI template.

Recommended Operations Verify which Template this VLAN interface has been bound in.

12427

Message Number 12427

Alarm Reason This Template hasn't bound with service.

Recommended Operations Bind Template with service.

12428

Message Number 12428

Alarm Reason This Template has been bound with a Vlan.

Recommended Operations Release the Template binding with other Vlan.

12429

Message Number 12429

Alarm Reason Management IP and FTP server IP are not configured.

Recommended Operations Configure Management IP and FTP server IP first.

12430

Message Number 12430

Alarm Reason This IP address has been bound with other FW or DPI board.

Recommended Operations Release the binding relationship between IP and other FW or DPI.

12431

Message Number 12431

Alarm Reason This entry has been configured.

Recommended Operations Delete this configuration first.

12432

Message Number 12432

Alarm Reason This entry hasn't been configured.

Recommended Operations Configure this entry first.

12433

Message Number 12433

Alarm Reason This service is bound with a Template.

Recommended Operations Release the Template binding with this service.

30201

Message Number 30201

Alarm Reason acl_ipv4_entrynum is empty. Basic acl and extended acl can't be configured to send to ESM at ESM_UDF mode.

Recommended Operations Please configure acl_ipv4_entrynum first to make it non-null.

30202

Message Number 30202

Alarm Reason acl_l2_entrynum is empty. Link acl can't be configured to send to ESM at ESM_UDF mode.

Recommended Operations Please configure acl_ l2_entrynum first to make it non-null.

30203

Message Number 30203

Alarm Reason acl_l2ipv4_entrynum is empty. Hybrid acl can't be configured to send to ESM at ESM_UDF mode.

Recommended Operations Please configure acl_ l2ipv4_entrynum first to make it non-null.

30204

Message Number 30204

Alarm Reason acl_ipv6c_entrynum is empty. Ipv6_standard acl can't be configured to send to ESM at ESM_UDF mode.

Recommended Operations Please configure acl_ipv6c_entrynum first to make it non-null.

30205

Message Number 30205

Alarm Reason acl_ipv6f_entrynum is empty. Ipv6_extendend acl can't be configured to send to ESM at ESM_UDF mode.

Recommended Operations Please configure acl_ipv6f_entrynum first to make it non-null.

30206

Message Number 30206

Alarm Reason At ESM_UDF mode, user configured entry number occupied ESM space has exceeded space of Sram or TCAM (TCAM space: 350MHz :521K, 500MHz 256K).

Recommended Operations	Clear or modify a entry size first to limit entry size in the specific space.

30207

Message Number	30207
Alarm Reason	TCAM with work frequency 350MHz doesn't support configuration of these entries.
Recommended Operations	Note TCAM type when it is configured.

30208

Message Number	30208
Alarm Reason	The deleting ACL mode of ESM configuration does not exist
Recommended Operations	Configure ESM acl mode first and then delete.

Chapter 4

TRAP Messages

Table of Contents

TRAP Message Explanation 257
System TRAP Message 257
Alarm TRAP Message 259
RMON TRAP Message 261
OSPF TRAP Message 262
BGP TRAP Message 271
DHCP TRAP Message 272
VRRP TRAP Message 273
IPv6TRAP Information 274
POE TRAP Information 274

TRAP Message Explanation

In the SNMP NMS, trap indicates a type of alarm report (similar to syslog report). Every trap has a trap type definition, which is used to indicate what type the alarm is (e.g.: LinkUp, LinkDown trap means link up and down alarms). Moreover, some traps can carry some binding variables for clearly describing the situation when alarm creating, e.g. the ifIndex bound in LinkUp and LinkDown traps is to indicate the interface index that LinkUp/LinkDown occurred (defined in RFC1213.MIB).

System TRAP Message

coldStart

Information Description The trap is sent during system power-on and starting.

Triggering Criteria
1. The system is been powered on and started.
2. The relevant configuration for SNMP sending trap is correct.

Recommended Operations None.

Binding variables None.

warmStart

Information Description The trap is sent when it reloads map start during system operation.

Triggering Criteria
1. System applies reload command to reload map initialization or main/standby switchover.
2. The relevant configuration for SNMP sending trap is correct.

Recommended Operations None.

Binding variables None.

authenticationFailure

Information Description The trap is sent when user password authentication is failed while SNMP v2 version is used to connect the equipment SNMP NMS.

Triggering Criteria
1. The user name and password are mismatched when SNMP v2 is used for accessing equipment.
2. The relevant configuration for SNMP sending trap is correct.

Recommended Operations Please check whether any equipment administrator is accessing the equipment; if it is, please check whether the user name and password are consistent with the relevant configuration on the equipment; if not, please check whether anybody is trying to monitor the equipment.

Binding variables None.

linkUp

Information Description The trap is sent when the interface changes from down to up (up in both the management status and operation status).

Triggering Criteria
1. The interface management and operation status both are in up.
2. The relevant configuration for SNMP sending trap is correct.

Recommended Operations None.

Binding variables ifIndex (interface index)

OID: 1.3.6.1.2.1.2.2.1.1

ifAdminStatus (interface managing status)

OID: 1.3.6.1.2.1.2.2.1.7

ifOperStatus (interface operating status)

OID: 1.3.6.1.2.1.2.2.1.8

linkDown

Information Description

The trap is sent when the interface changes from up to down (it might be the managing status is down and the operating status is down, or, both changed from up to down).

Triggering Criteria

1. The interface operating status changes from up to down, or the managing status changes from up to down.
2. The relevant configuration for SNMP sending trap is correct.

Recommended Operations

Please check whether the system is running normally and the interface connection cable is well.

Binding variables

ifIndex (interface index)

OID: 1.3.6.1.2.1.2.2.1.1

ifAdminStatus (interface managing status)

OID: 1.3.6.1.2.1.2.2.1.7

ifOperStatus (interface operating status)

OID: 1.3.6.1.2.1.2.2.1.8

Alarm TRAP Message

Hardware Alarm Trap

Information Description

The trap is sent when a hardware alarm occurs on equipment.

Triggering Criteria

1. A hardware-related alarm occurs on equipment.
2. The equipment is configured the unm on and unm server commands.
3. The relevant configuration for SNMP sending trap is correct.

Recommended Operations

Please find the corresponding operation recommendation according to the alarm code bound in alarm trap.

Binding variables

Rack No., value 1

OID: 1.3.6.1.4.1.3902.3.4.6.1.1

Shelf No., value 1

OID: 1.3.6.1.4.1.3902.3.4.6.1.2

Slot number

OID: 1.3.6.1.4.1.3902.3.4.6.1.3

Port No., value 0 if no corresponding port existed

OID: 1.3.6.1.4.1.3902.3.4.6.1.4

Alarm Code

OID: 1.3.6.1.4.1.3902.3.4.6.1.5

Alarm Severe level

OID: 1.3.6.1.4.1.3902.3.4.6.1.6

Alarm generation time

OID: 1.3.6.1.4.1.3902.3.4.6.1.7

Alarm status: alarm created, alarm cleared

OID: 1.3.6.1.4.1.3902.3.4.6.1.8

Alarm type: environment alarm 1, line card alarm 2, port alarm 3

OID: 1.3.6.1.4.1.3902.3.4.6.1.9

Alarm variable value, 0 as no

OID: 1.3.6.1.4.1.3902.3.4.6.1.10

Alarm upper variable value, 0 as no

OID: 1.3.6.1.4.1.3902.3.4.6.1.11

Alarm lower variable value, 0 as no

OID: 1.3.6.1.4.1.3902.3.4.6.1.12

Alarm description message

OID: 1.3.6.1.4.1.3902.3.4.6.1.13

Software Alarm Trap

Information Description

The trap is sent when a software alarm occurs on equipment.

Triggering Criteria

1. A software alarm occurs on equipment.
2. It configures unm on and unm server commands.
3. The relevant configuration for SNMP sending trap is correct.

Recommended Operations

Please find the corresponding operation recommendation according to the alarm code bound in the alarm trap.

Binding variables

Rack No., value 1

OID: 1.3.6.1.4.1.3902.3.4.7.1.1

Shelf No., value 1

OID: 1.3.6.1.4.1.3902.3.4.7.1.2

Slot number

OID: 1.3.6.1.4.1.3902.3.4.7.1.3

Alarm Code

OID: 1.3.6.1.4.1.3902.3.4.7.1.4

Alarm Severe level

OID: 1.3.6.1.4.1.3902.3.4.7.1.5

Alarm generation time

OID: 1.3.6.1.4.1.3902.3.4.7.1.6

Alarm status: alarm created

OID: 1.3.6.1.4.1.3902.3.4.7.1.7

Alarm Type: ros 65, database 66 …

OID: 1.3.6.1.4.1.3902.3.4.7.1.8

Alarm description message

OID: 1.3.6.1.4.1.3902.3.4.7.1.9

RMON TRAP Message

Syntax

risingAlarm Trap

Information Description

The trap is sent when the monitored variable on RMON alarm table exceeds the set upper alarm limit.

Triggering Criteria

1. The monitored alarm variable value exceeds the set upper alarm limit.
2. The trap sending is defined in the corresponding rising event control item in the alarm control item.
3. The relevant configuration for SNMP sending trap is correct.

Recommended Operations

Please take the corresponding measure according to the influence of the monitored variable changes on the system.

Binding variables

alarmIndex (alarm control table item index No.)

OID: 1.3.6.1.2.1.16.3.1.1.1

alarmVariable (monitored alarm variable)

OID: 1.3.6.1.2.1.16.3.1.1.3

alarmSampleType (monitored variable value sampling type: absolute value type, difference type)

OID: 1.3.6.1.2.1.16.3.1.1.4

alarmValue (monitored variable value)

OID: 1.3.6.1.2.1.16.3.1.1.5

alarmRisingThreshold (set upper threshold of monitored variable)

OID: 1.3.6.1.2.1.16.3.1.1.7

fallingAlarm Trap

Information Description

The trap is sent when the monitored variable in RMON alarm table is lower than the set lower alarm limit.

Triggering Criteria

1. The monitored alarm variable is lower than set lower alarm limit.
2. The trap sending is defined in the corresponding falling event control item in the alarm control item.
3. The relevant configuration for SNMP sending trap is correct.

Recommended Operations

Please take the corresponding measure according to the influence of the monitored variable changes on the system.

Binding variables

alarmIndex (alarm control table item index No.)

OID: 1.3.6.1.2.1.16.3.1.1.1

alarmVariable (monitored alarm variable)

OID: 1.3.6.1.2.1.16.3.1.1.3

alarmSampleType (monitored variable value sampling type: absolute value type, difference type)

OID: 1.3.6.1.2.1.16.3.1.1.4

alarmValue (monitored variable value)

OID: 1.3.6.1.2.1.16.3.1.1.5

alarmFallingThreshold (set lower threshold of monitored variable)

OID: 1.3.6.1.2.1.16.3.1.1.8

OSPF TRAP Message

Syntax

ospfVirtIfStateChange

Information Description

The trap is sent when OSPF virtual interface status is changed.

Triggering Criteria

1. OSPF virtual interface status is changed.
2. The relevant configuration for SNMP sending trap is correct.

Recommended Operations

Please check whether OSPF virtual interface status change is normal; if not, please check whether the router interface status related to OSPF virtual interface is normal, and the router OSPF configuration (and the OSPF configuration of neighbors related to OSPF) is normal; if the fault remained, please contact ZTE.

Binding variables

ospfRouterId (router ID used to distinguish the routers in autonomous system, and the value is only value)

OID: 1.3.6.1.2.1.14.1.1

ospfVirtIfAreaId (the area ID crossed by OSPF virtual connection)

OID: 1.3.6.1.2.1.14.9.1.1

ospfVirtIfNeighbor (the router ID of OSPF virtual neighbor)

OID: 1.3.6.1.2.1.14.9.1.2

ospfVirtIfState (OSPF virtual interface status)

OID: 1.3.6.1.2.1.14.9.1.7

ospfNbrStateChange

Information Description

OSPF non-virtual neighbor status change

Triggering Criteria

1. OSPF non-virtual neighbor status change may be to normal direction, or may be the status regress caused by abnormal cases.
2. The configuration for SNMP-related OSPF sending trap is correct.

Recommended Operations

Please check whether OSPF neighbor status change is normal, if not, check whether the router system is running normally, and whether the link connection is normal.

Binding variables

ospfRouterId (router ID used to distinguish the routers in autonomous system, and the value is only value)

OID: 1.3.6.1.2.1.14.1.1

ospfNbrIpAddr (OSPF neighbor interface IP address, which might be another interface address in connection without address)

OID: 1.3.6.1.2.1.14.10.1.1

ospfNbrAddressLessIndex (the IP address index on interface mib table, which corresponding to OSPF neighbor interface)

OID: 1.3.6.1.2.1.14.10.1.2

ospfNbrRtrId (the router ID of OSPF neighbor router)

OID: 1.3.6.1.2.1.14.10.1.3

ospfNbrState (OSPF neighbor status)

OID: 1.3.6.1.2.1.14.10.1.6

ospfVirtNbrStateChange

Information Description

OSPF virtual neighbor status change.

Triggering Criteria

1. OSPF virtual neighbor status change may be to normal direction, or may be the status regress caused by abnormal cases.
2. The configuration for SNMP-related OSPF sending trap is correct.

Recommended Operations

Please check whether OSPF virtual neighbor status change is normal, if not, check whether the router system is running normally, and whether the link connection is normal.

Binding variables

ospfRouterId (router ID used to distinguish the routers in autonomous system, and the value is only value)

OID: 1.3.6.1.2.1.14.1.1

ospfVirtNbrArea (the area crossed by OSPF virtual neighbor)

OID: 1.3.6.1.2.1.14.11.1.1

ospfVirtNbrRtrId (the router ID of OSPF virtual neighbor)

OID: 1.3.6.1.2.1.14.11.1.2

ospfVirtNbrState (OSPF virtual neighbor status)

OID: 1.3.6.1.2.1.14.11.1.5

ospfIfConfigError

Information Description

Incorrect OSPF non-virtual interface configuration

Triggering Criteria

1. The peer parameter configuration at OSPF non-virtual interface is inconsistent with the relevant configuration of the router.
2. The configuration for SNMP-related OSPF sending trap is correct.

Recommended Operations

Please check whether the router configurations related to OSPF protocol are consistent with the opposite end.

Binding variables

ospfRouterId (router ID used to distinguish the routers in autonomous system, and the value is only value)

OID: 1.3.6.1.2.1.14.1.1

ospfIfIpAddress (the IP address at OSPF interface)

OID: 1.3.6.1.2.1.14.7.1.1

ospfAddressLessIf (index of interface without address, 0 for interface with address and ifIndex index for interface without address)

OID: 1.3.6.1.2.1.14.7.1.2

ospfPacketSrc (OSPF report IP address unable to be identified by neighbor example)

OID: 1.3.6.1.2.1.14.16.1.4

ospfConfigErrorType (the possible types of OSPF configuration errors, as error version number, mismatched area number and unknown virtual neighbor)

OID: 1.3.6.1.2.1.14.16.1.2

ospfPacketType (OSPF packet type: hello packet, lsReq packet, and lsAck packet)

OID: 1.3.6.1.2.1.14.16.1.3

ospfVirtIfConfigError

Information Description

Error OSPF virtual interface configuration

Triggering Criteria

1. The peer parameter configuration at OSPF virtual interface is inconsistent with the relevant configuration of the router.
2. The configuration for SNMP-related OSPF sending trap is correct.

Recommended Operations

Please check whether the router configurations related to OSPF protocol are consistent with the opposite end.

Binding variables

ospfRouterId (router ID used to distinguish the routers in autonomous system, and the value is only value)

OID: 1.3.6.1.2.1.14.1.1

ospfVirtIfAreaId (the area ID crossed by OSPF virtual connection)

OID: 1.3.6.1.2.1.14.9.1.1

ospfVirtIfNeighbor (the router ID of OSPF virtual neighbor)

OID: 1.3.6.1.2.1.14.9.1.2

ospfConfigErrorType (the possible types of OSPF configuration errors, as error version number, mismatched area number and unknown virtual neighbor)

OID: 1.3.6.1.2.1.14.16.1.2

ospfPacketType (OSPF packet type: hello packet, lsReq packet, and lsAck packet)

OID: 1.3.6.1.2.1.14.16.1.3

ospfIfAuthFailure

Information Description

The authentication type or key of OSPF report received at non-virtual interface is inconsistent with the relevant configuration of the router, which causes the authentication failure.

Triggering Criteria

1. The authentication type or key of OSPF report received at non-virtual interface is inconsistent with the relevant configuration of the router.
2. The SNMP configuration about OSPF trap sending is correct.

Recommended Operations

Please check whether the router configuration is consistent with the one about OSPF at the opposite end router.

Binding variables

ospfRouterId (router ID used to distinguish the routers in autonomous system, and the value is only value)

OID: 1.3.6.1.2.1.14.1.1

ospfIfIpAddress (the IP address at OSPF interface)

OID: 1.3.6.1.2.1.14.7.1.1

ospfAddressLessIf (index of interface without address, 0 for interface with address and ifIndex index for interface without address)

OID: 1.3.6.1.2.1.14.7.1.2

ospfPacketSrc (OSPF report IP address unable to be identified by neighbor example)

OID: 1.3.6.1.2.1.14.16.1.4

ospfConfigErrorType (the possible types of OSPF configuration errors, as error version number, mismatched area number and unknown virtual neighbor)

OID: 1.3.6.1.2.1.14.16.1.2

ospfPacketType (OSPF packet type: hello packet, lsReq packet, and lsAck packet)

OID: 1.3.6.1.2.1.14.16.1.3

ospfVirtIfAuthFailure

Information Description

The authentication type or key of OSPF report received at virtual interface is inconsistent with the relevant configuration of the router, which causes the authentication failure.

Triggering Criteria

1. The authentication type or key of OSPF report received at OSPF virtual interface is inconsistent with the relevant configuration of the router.
2. The SNMP configuration about OSPF trap sending is correct.

Recommended Operations

Please check whether the router configuration is consistent with the one about OSPF at the opposite end router.

Binding variables

ospfRouterId (router ID used to distinguish the routers in autonomous system, and the value is only value)

OID: 1.3.6.1.2.1.14.1.1

ospfVirtIfAreaId (the area ID crossed by OSPF virtual connection)

OID: 1.3.6.1.2.1.14.9.1.1

ospfVirtIfNeighbor (the router ID of OSPF virtual neighbor)

OID: 1.3.6.1.2.1.14.9.1.2

ospfConfigErrorType (the possible types of OSPF configuration errors, as error version number, mismatched area number and unknown virtual neighbor)

OID: 1.3.6.1.2.1.14.16.1.2

ospfPacketType (OSPF packet type: hello packet, lsReq packet, and lsAck packet)

OID: 1.3.6.1.2.1.14.16.1.3

ospfIfRxBadPacket

Information Description

Fail to resolute OSPF report received at OSPF non-virtual interface.

Triggering Criteria

1. Fail to resolute OSPF report received at OSPF non-virtual interface.
2. The SNMP configuration about OSPF trap sending is correct.

Recommended Operations

Please check whether the link between routers is perfect and the router configuration at two sides is consistent, correct and proper.

Binding variables

ospfRouterId (router ID used to distinguish the routers in autonomous system, and the value is only value)

OID: 1.3.6.1.2.1.14.1.1

ospfIfIpAddress (the IP address at OSPF interface)

OID: 1.3.6.1.2.1.14.7.1.1

ospfAddressLessIf (index of interface without address, 0 for interface with address and ifIndex index for interface without address)

OID: 1.3.6.1.2.1.14.7.1.2

ospfPacketSrc (OSPF report IP address unable to be identified by neighbor example)

OID: 1.3.6.1.2.1.14.16.1.4

ospfPacketType (OSPF packet type: hello packet, lsReq packet, and lsAck packet)

OID: 1.3.6.1.2.1.14.16.1.3

ospfVirtIfRxBadPacket

Information Description

Fail to resolute OSPF report received at OSPF virtual interface.

Triggering Criteria

1. Fail to resolute OSPF report received at OSPF virtual interface.
2. The SNMP configuration about OSPF trap sending is correct.

Recommended Operations

Please check whether the link between routers is perfect and the router configurations at two sides are consistent, correct and proper.

Binding variables

ospfRouterId (router ID used to distinguish the routers in autonomous system, and the value is only value)

OID: 1.3.6.1.2.1.14.1.1

ospfVirtIfAreaId (the area ID crossed by OSPF virtual connection)

OID: 1.3.6.1.2.1.14.9.1.1

ospfVirtIfNeighbor (the router ID of OSPF virtual neighbor)

OID: 1.3.6.1.2.1.14.9.1.2

ospfPacketType (OSPF packet type: hello packet, lsReq packet, and lsAck packet)

OID: 1.3.6.1.2.1.14.16.1.3

ospfTxRetransmit

Information Description

OSPF report is transferred on OSPF non-virtual interface.

Triggering Criteria

1. The report received at the OSPF non-virtual interface is transferred.
2. The SNMP configuration about OSPF trap sending is correct.

Recommended Operations

None

Binding variables

ospfRouterId (router ID used to distinguish the routers in autonomous system, and the value is only value)

OID: 1.3.6.1.2.1.14.1.1

ospfIfIpAddress (the IP address at OSPF interface)

OID: 1.3.6.1.2.1.14.7.1.1

ospfAddressLessIf (index of interface without address, 0 for interface with address and ifIndex index for interface without address)

OID: 1.3.6.1.2.1.14.7.1.2

ospfNbrRtrId (the router ID of OSPF neighbor router)

OID: 1.3.6.1.2.1.14.10.1.3

ospfPacketType (OSPF packet type: hello packet, lsReq packet, and lsAck packet)

OID: 1.3.6.1.2.1.14.16.1.3

ospfLsdbType (link status broadcast type: router link, network link, and group broadcast link)

OID: 1.3.6.1.2.1.14.4.1.2

ospfLsdbLsid (link status ID, formed by router ID or IP address)

OID: 1.3.6.1.2.1.14.4.1.3

ospfLsdbRouterId (router ID originating link status broadcast report)

OID: 1.3.6.1.2.1.14.4.1.4

ospfVirtIfTxRetransmit

Information Description

OSPF report is transferred on OSPF non-virtual interface.

Triggering Criteria

1. The report received at the OSPF non-virtual interface is transferred.
2. The SNMP configuration about OSPF trap sending is correct.

Recommended Operations

None.

Binding variables

ospfRouterId (router ID used to distinguish the routers in autonomous system, and the value is only value)

OID: 1.3.6.1.2.1.14.1.1

ospfVirtIfAreaId (the area ID crossed by OSPF virtual connection)

OID: 1.3.6.1.2.1.14.9.1.1

ospfVirtIfNeighbor (the router ID of OSPF virtual neighbor)

OID: 1.3.6.1.2.1.14.9.1.2

ospfPacketType (OSPF packet type: hello packet, lsReq packet, and lsAck packet)

OID: 1.3.6.1.2.1.14.16.1.3

ospfLsdbType (link status broadcast type: router link, network link, and group broadcast link)

OID: 1.3.6.1.2.1.14.4.1.2

ospfLsdbLsid (link status ID, formed by router ID or IP address)

OID: 1.3.6.1.2.1.14.4.1.3

ospfLsdbRouterId (router ID originating link status broadcast report)

OID: 1.3.6.1.2.1.14.4.1.4

ospfOriginateLsa

Information Description

The router creates a new link status broadcast report.

Triggering Criteria

1. The router creates a link status broadcast report because of the topology change of the autonomous domain where the router is in.
2. The SNMP configuration about OSPF trap sending is correct.

Recommended Operations

Please check whether the topology status change in autonomous domain is normal.

Binding variables

ospfRouterId (router ID used to distinguish the routers in autonomous system, and the value is only value)

OID: 1.3.6.1.2.1.14.1.1

ospfLsdbAreaId (the area ID of router, value 0.0.0.0 for outside of autonomous system)

OID: 1.3.6.1.2.1.14.4.1.1

ospfLsdbType (link status broadcast type: router link, network link, and group broadcast link)

OID: 1.3.6.1.2.1.14.4.1.2

ospfLsdbLsid (link status ID, formed by router ID or IP address)

OID: 1.3.6.1.2.1.14.4.1.3

ospfLsdbRouterId (router ID originating link status broadcast report)

OID: 1.3.6.1.2.1.14.4.1.4

ospfMaxAgeLsa

Information Description

LSA reaches the maximum aging time on router link status database.

Triggering Criteria

1. LSA reaches the maximum aging time on router link status database.
2. The SNMP configuration about OSPF trap sending is correct.

Recommended Operations

None.

Binding variables

ospfRouterId (router ID used to distinguish the routers in autonomous system, and the value is only value)

OID: 1.3.6.1.2.1.14.1.1

ospfLsdbAreaId (the area ID of router, value 0.0.0.0 for outside of autonomous system)

OID: 1.3.6.1.2.1.14.4.1.1

ospfLsdbType (link status broadcast type: router link, network link, and group broadcast link)

OID: 1.3.6.1.2.1.14.4.1.2

ospfLsdbLsid (link status ID, formed by router ID or IP address)

OID: 1.3.6.1.2.1.14.4.1.3

ospfLsdbRouterId (router ID originating link status broadcast report)

OID: 1.3.6.1.2.1.14.4.1.4

ospfLsdbOverflow

Information Description

LSA database overflow trap

Triggering Criteria

1. LSA quantity on link status database exceeds the maximum value of the external link status database.
2. The SNMP configuration about OSPF trap sending is correct.

Recommended Operations

Check whether the router configuration is proper and the permitted router performance parameters are applicable to the autonomous domain division.

Binding variables

ospfRouterId (router ID used to distinguish the routers in autonomous system, and the value is only value)

OID: 1.3.6.1.2.1.14.1.1

ospfExtLsdbLimit (the maximum non-default external LSA quantity able to store on link status database)

OID: 1.3.6.1.2.1.14.1.11

ospfLsdbApproachingOverflow

Information Description

LSA quantity on link status database exceeds 90% of maximum external link status database value.

Triggering Criteria

1. LSA quantity on link status database exceeds 90% of maximum external link status database value.
2. The SNMP configuration about OSPF trap sending is correct.

Recommended Operations

Please check whether the autonomous domain system operation is normal, the router configuration is proper and the permitted router performance parameters is applicable to the autonomous domain division.

Binding variables

ospfRouterId (router ID used to distinguish the routers in autonomous system, and the value is only value)

OID: 1.3.6.1.2.1.14.1.1

ospfExtLsdbLimit (the maximum non-default external LSA quantity able to store on link status database)

OID: 1.3.6.1.2.1.14.1.11

ospfIfStateChange

Information Description OSPF non-virtual interface status change

Triggering Criteria
1. OSPF non-virtual interface status change
2. The SNMP configuration about OSPF trap sending is correct.

Recommended Operations Please check whether OSPF non-virtual interface status changes are to the correct direction; if not, check if the link connection status and router operation are normal please.

Binding variables ospfRouterId (router ID used to distinguish the routers in autonomous system, and the value is only value)

OID: 1.3.6.1.2.1.14.1.1

ospfIfIpAddress (the IP address at OSPF interface)

OID: 1.3.6.1.2.1.14.7.1.1

ospfAddressLessIf (index of interface without address, 0 for interface with address and ifIndex index for interface without address)

OID: 1.3.6.1.2.1.14.7.1.2

ospfVirtIfState (OSPF interface status)

OID: 1.3.6.1.2.1.14.7.1.12

BGP TRAP Message

bgpEstablished

Information Description BGP state machine status is changed to ESTABLISHED status.

Triggering Criteria
1. BGP state machine status is changed to ESTABLISHED status.
2. The SNMP configuration about BGP trap sending is correct.

Recommended Operations None.

Binding variables bgpPeerLastError (error number and sub-number appeared on BGP peer; value 0 if no error)

OID: 1.3.6.1.2.1.15.3.1.14

bgpPeerState (BGP peer status, as idle, connect, and active)

OID: 1.3.6.1.2.1.15.3.1.2

bgpBackwardTransition

Information Description The trap indicates that BGP state machine regresses from high-level status to lower-level status.

Triggering Criteria

1. BGP state machine status is changed from high-level status to lower-level status.
2. The SNMP configuration about BGP trap sending is correct.

Recommended Operations

Please check if the routers at both peer sides are running normally, the link connection status is normal; and if it is caused by improper router protocol configuration modification.

Binding variables

bgpPeerLastError (error number and sub-number appeared on BGP peer; value 0 if no error)

OID: 1.3.6.1.2.1.15.3.1.14

bgpPeerState (BGP peer status, as idle, connect, and active)

OID:1.3.6.1.2.1.15.3.1.2

DHCP TRAP Message

online

Information Description

The trap message sent when DHCP user gets online.

Triggering Criteria

1. DHCP user gets online.
2. SNMP configuration for sending trap is correct.

Recommended Operations

No.

Binding variables

No.

offline

Information Description

The trap message sent when DHCP user gets offline.

Triggering Criteria

1. DHCP user gets offline.
2. SNMP configuration for sending trap is correct.

Recommended Operations

No.

Binding variables No.

VRRP TRAP Message

vrrpTrapAuthFailure

Information Description Vrrp authentication is failure.

Triggering Criteria
1. The authentication message received vrrp and the set authentication message is not the same.
2. SNMP configuration about vrrp sending trap is correct.

Recommended Operations Check whether the packet authentication message between the main and the backup routers is the same. If they need to communicate with each other, then the authentication message must be the same.

Binding variables vrrpTrapPacketSrc(The source address of vrrp packet)

OID: 1, 3, 6, 1, 2, 1, 68, 1, 5, 0

vrrpTrapAuthErrorType(vrrp authentication failure type)

vrrp authentication failure type: VRRP_AUTH_TYPE_INVALID 1

VRRP_AUTH_TYPE_MISMATCH 2

VRRP_AUTH_FAIL 3

OID1, 3, 6, 1, 2, 1, 68, 1, 6, 0

vrrpTrapNewMaster

Information Description Vrrp active turns into standby.

Triggering Criteria
1. VRRP active and standby changeover.
2. VRRP priority changes.

Recommended Operations Check whether the system is steady after the active and the standby changeover.

Binding variables vrrpOperMasterIpAddr(the virtual IP address, when the active turns into standby)

OID: 1, 3, 6, 1, 2, 1, 68, 1, 3, 1, 7, 0, 0

IPv6TRAP Information

ipv6IfStateChange

Message Description IPv6 interface status changes.

Trigger Conditions
1. IPv6 interface status changes.
2. The configuration of SNMP related to Ipv6 sending trap is correct.

Recommended Operations N.A.

Bound Variables

ipv6IfDescr Ipv6 interface description

OID 1.3.6.1.2.1.55.1.5.1.2

ipv6IfOperStatus (IPv6 interface operation status)

OID 1.3.6.1.2.1.55.1.5.1.10

IPv6 interface operation status type:

up 1

down 2

noIfIdentifier 3

unknown 4

notPresent 5

POE TRAP Information

pethPsePortOnOffNotification

Message Description The port PoE power supply status is changing.

Trigger Conditions
1. The port PoE power supply status is changing.
2. The configuration of SNMP related to PoE sending trap is correct.

Recommended Operations N.A.

Bound Variables

pethPsePortGroupIndex PSE device number

OID 1.3.6.1.2.1.105.1.1.1.1

pethPsePortIndex (Port index)

OID 1.3.6.1.2.1.105.1.1.1.2

pethPsePortDetectionStatus (Port PoE power supply status)

OID 1.3.6.1.2.1.105.1.1.1.6

The port PoE power supply status type:

disabled 1

searching 2

deliveringPower 3

fault 4

test 5

otherFault 6

pethMainPowerUsageOnNotification

Message Description PSE total power of the power supply exceeds power threshold.

Trigger Conditions
1. PSE total power of the power supply exceeds power threshold.
2. The configuration of SNMP related to PoE sending trap is correct.

Recommended Operations N.A.

Bound Variables

pethMainPseGroupIndex PSE device number

OID 1.3.6.1.2.1.105.1.3.1.1.1

pethMainPseConsumptionPower PSE total power of power supply

OID 1.3.6.1.2.1.105.1.3.1.1.4

pethMainPseUsageThreshold PSE power threshold

OID 1.3.6.1.2.1.105.1.3.1.1.5

pethMainPowerUsageOffNotification

Message Description PSE total power of the power supply recovers in the range of power threshold.

Trigger Conditions
1. PSE total power of the power supply exceeds power threshold or recovers in the range of power threshold.
2. The configuration of SNMP related to PoE sending trap is correct.

Recommended Operations N.A.

Bound Variables

pethMainPseGroupIndex PSE device number

OID 1.3.6.1.2.1.105.1.3.1.1.1

pethMainPseConsumptionPower PSE total power of power supply

OID 1.3.6.1.2.1.105.1.3.1.1.4

pethMainPseUsageThreshold PSE power threshold

OID 1.3.6.1.2.1.105.1.3.1.1.5